

# Fortra's GoAnywhere Managed File Transfer v6.8 Common Criteria Configuration Guide

---

Document Version: 1.1



2400 Research Blvd  
Suite 395  
Rockville, MD 20850

## Contents

1	Purpose of this document.....	5
1.1	TOE Overview.....	5
2	TOE Description.....	5
2.1	Evaluated Configuration .....	5
2.1.1	<b>Operational Environment.....</b>	<b>5</b>
2.2	Physical Boundaries .....	6
2.3	Logical Boundaries .....	6
2.4	Other Assumptions .....	7
2.5	Excluded Functionality and Configuration .....	8
3	Secure Installation and Configuration .....	9
3.1	Prerequisites .....	10
3.2	Installing GoAnywhere MFT.....	11
4	Platform Security and Cryptography.....	13
4.1	Initial Configurations.....	13
4.2	Enabling FIPS 140-2 mode.....	13
4.3	Certificate Validation .....	14
4.4	Hostname Verification .....	15
4.5	SSL/TLS configuration.....	16
5	Setting up secure communication .....	18
5.1	Database Configuration .....	18
5.2	Authentication Server Configuration .....	22
5.3	Admin Server Configuration.....	27
5.4	HTTPS Server Configuration .....	33
5.5	SFTP Server Configuration .....	37
5.6	SFTP Client Configuration .....	42
5.7	Mail Server Configuration .....	47
5.8	Workflows and Projects .....	49
6	Management Functions .....	50
6.1	Configuring Various System Users: .....	50
6.2	Configure Keys and Certificates: .....	56
7	Secure Updates .....	60
8	TOE access to platform resources.....	60

9	References .....	61
---	------------------	----

## Revision History

Version	Date	Changes
1.0	December 29, 2022	Initial Release
1.1	March 29, 2023	Minor update

# 1 Purpose of this document

This document is a guide for the Fortra's GoAnywhere Managed File Transfer v6.8 (MFT) implementation of the Common Criteria Application Protection Profile v1.3 (SWAPP v1.3). The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the GoAnywhere MFT 6.8

This document will guide how to install, configure, and operate the Application in a Common Criteria Compliant mode.

- How to install GoAnywhere MFT 6.8 on Windows server 2016 and CentOS7
- The secure communication mechanisms employed by GoAnywhere MFT 6.8
- How to update the GoAnywhere MFT 6.8

## 1.1 TOE Overview

The Target of Evaluation (TOE) is the Fortra's GoAnywhere Managed File Transfer v6.8 (MFT). The TOE is a software application that provides secure file transfer services over HTTPS, TLS, and SSH. GoAnywhere MFT is a secure managed file transfer solution that streamlines the exchange of data between systems, employees, customers, and trading partners. It provides centralized control with extensive security settings, detailed audit trails, and helps process information from files into XML, CSV, and JSON databases.

# 2 TOE Description

## 2.1 Evaluated Configuration

The TOE has been evaluated on the following host platforms:

- CentOS 7 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)
- Windows Server 2016 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)

Note: The TOE is the application software only. The host platforms are not part of the evaluation.

### 2.1.1 Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration. The TOE supports (sometimes optionally) secure connectivity with several other IT environment devices as described below.

Environment Component	Required	Usage/Purpose Description
Web Browser	Yes	Remote administration and User file access over TLSv1.2.

Environment Component	Required	Usage/Purpose Description
Database Server	Yes	MySQL, MS SQL Server, Oracle, or DB2/400 for storing settings. The server must support TLSv1.2 to enable secure access by the TOE.
LDAP/AD Server	No	Remote authentication server supporting TLSv1.2.
Mail Server	No	Mail server supporting SMTP over TLSv1.2 for sending notifications.
File Server	No	Remote file server for storing user files: <ul style="list-style-type: none"> <li>• AS2, AS4, or WebDAV servers supporting HTTPS/TLSv1.2</li> <li>• SFTP or SCP servers supporting SSHv2</li> <li>• FTP/s servers supporting TLSv1.2</li> <li>• Amazon S3 or Azure Blob Storage supporting HTTPS/TLSv1.2</li> <li>• REST, SOAP, or generic HTTPS server</li> </ul>
File Transfer Client	No	Client allowing users to store and retrieve files from the TOE: <ul style="list-style-type: none"> <li>• AS2 or AS4 clients supporting HTTPS/TLSv1.2</li> <li>• SFTP or SCP clients supporting SSHv2</li> <li>• FTP/s client supporting TLSv1.2</li> </ul>
CRL Server	Yes	Server which contains updated revocation list for the TOE.
Java Runtime Environment	Yes (on CentOS)	Platform-provided Java SE 8 Java Runtime Environment (JRE). Note: The Windows platform does not provide a JRE, so the Windows version of the TOE includes the required JRE.

Table 1 IT Environment Components

## 2.2 Physical Boundaries

The TOE is a software application running on a host platform (as listed above).

## 2.3 Logical Boundaries

The TOE provides the security functionality required by [SWAPP], [TLS-PKG], and [SSH-EP]. The TOE consists of the Fortra Java Software, JVM, Tomcat, Bouncy Castle crypto module, JSCH client (SSHC), Jadaptive (SSHS).

### Cryptographic Support

The TOE utilizes the GoAnywhere MFT Bouncy Castle FIPS Java API cryptographic library version 1.0.2. This library implements all the cryptographic algorithms required for SSH and TLS, drawing entropy from the platform RBG.

The cryptographic services provided by the TOE are described below.

Cryptographic Protocol	Use within the TOE
SSHv2 Client	File server transfers using SFTP or SCP

Cryptographic Protocol	Use within the TOE
SSHv2 Server	User file transfers using SFTP or SCP
TLSv1.2 Client	Database server; Authentication Server; Mail Server; File server transfers using AS2, AS4, WebDAV, FTP/s, Amazon S3, Azure Blob Storage, REST, SOAP, or HTTPS; Check for updates
TLSv1.2 Server	HTTPS Remote administration; HTTPS file access; User file transfers using AS2, AS4, FTP/s
TLSv1.2 Client	Database server; Authentication Server; Mail Server;
TLSv1.2 Server	User file transfers using FTP/s

Table 2 TOE Provided Cryptography

## 2.4 Other Assumptions

### User Data Protection

The TOE relies on the underlying platform to encrypt sensitive data at rest.

### Identification and Authentication

The TOE uses X.509v3 certificates as defined by RFC 5280 to authentication the TLS connection to the external TLS servers. The TOE validates the X.509 certificates using the certificate path validation algorithm defined in RFC 5280.

The TOE authenticates users using a username/password combination or X.509 TLS Client Certificates.

### Security Management

The TOE allows the configuration of users, database server, authentication server, mail server, file servers, file transfer services, keys and certificates, and cryptographic protocols.

### Privacy

The TOE does not transmit Personally Identifiable Information (PII) over the network.

### Protection of TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE only allocates a limited amount of memory with both write and execute permission to support just-in-time compiling. The TOE supports ASLR, stack-based overflow protections, and platform security mechanisms (Windows Defender and SELinux).

The TOE is distributed as a Microsoft .EXE file (Windows) or an RPM (CentOS). The installers are signed by Fortra so their integrity can be verified by the platform.

### Trusted path/channels

The TOE protects all data in transit using TLSv1.2 or SSHv2.

## 2.5 Excluded Functionality and Configuration

The TOE includes the following functionality that is not covered as a part of the Common Criteria evaluation and no assurance as to the correct operation is provided. Therefore, it is recommended not to enable or configure the following resources available at Resources Tab as a part of Common Criteria Evaluated Configuration.

### Cloud Connectors

It is recommended to not enable or configure cloud connectors as this functionality is not tested as a part of the evaluation.

### FTP Servers

It is recommended to not enable or configure FTP servers as this functionality tend to transfer files over unencrypted channels without any secure communication and is not the part of the evaluation.

### Go Fast Servers

It is recommended to not enable or configure Go Fast Servers as this functionality was not tested as a part of the Common Criteria evaluation.

### HTTP Servers

It is recommended to not enable or configure HTTP servers as this functionality does transfer of data in plain text without any secure communication and is not the part of the evaluation.

### IBM i Servers

It is recommended to not enable or configure IBM i servers as this functionality is not tested as a part of the Common Criteria evaluation.

### ICAP Servers

It is recommended to not enable or configure ICAP servers as this functionality is not tested as a part of the Common Criteria evaluation.

### Mailboxes

It is recommended to not enable or configure Mailboxes as this functionality is not tested as a part of the Common Criteria evaluation.

### MQ Servers

It is recommended to not enable or configure MQ servers as this functionality is not tested as a part of the Common Criteria evaluation.

### Network Shares

It is recommended to not enable or configure Network Shares as this functionality is not tested as a part of the Common Criteria evaluation.

### PeSIT Servers

It is recommended to not enable or configure PeSIT Servers as this functionality is not tested as a part of the Common Criteria evaluation.



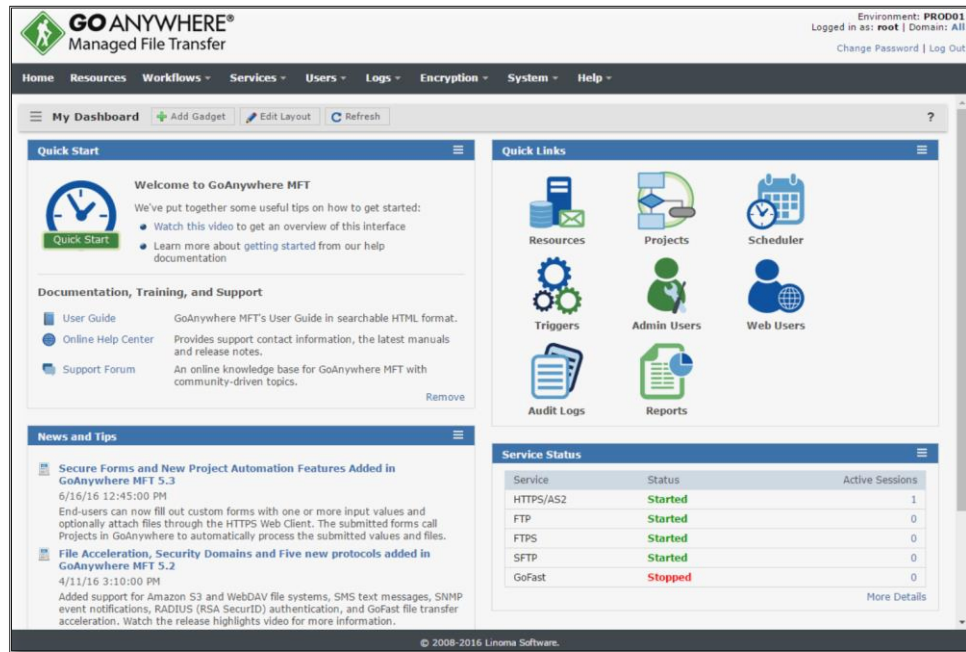
#### SNMP Servers

It is recommended to not enable or configure SNMP Servers as this functionality is not tested as a part of the Common Criteria evaluation.

### **3** Secure Installation and Configuration

### 3.1 Prerequisites

Authorized users can utilize GoAnywhere's browser-based Administrator to perform configuration and monitoring within the product.



#### Port Number Usage

Listed below are the default port numbers that will be used for GoAnywhere modules. These port numbers can be overridden during the installation or at any time after the installation. You may need to adjust your firewall settings or other access control software to allow connections on these ports.

Port Number	Description
8001	Administrator functions over HTTPS
8005	Shutdown port for GoAnywhere
443	HTTPS/AS2 service for trading partners
22	SFTP service for trading partners

#### Browser Compatibility

The GoAnywhere Administrator and Web Client interface's require modern internet browsers that support HTML 5. Popular browsers are supported including Internet Explorer\*, Edge, Chrome, Firefox and Safari. Please note that some HTML 5 advanced features, such as drag and drop, will not work in older versions of browsers.

\*GoAnywhere MFT supports Microsoft Internet Explorer 9, 10, and 11.

#### Installing GoAnywhere in a Virtual Environment

GoAnywhere MFT can be installed in most virtual environments. When installing in a virtual environment, the MAC address on the server where GoAnywhere is installed must be static. Your GoAnywhere MFT license will become invalid if the MAC addresses changes, and a new license must be issued by contacting Fortra Sales.

For Pre-Installation notes please click on the link below and refer to Page 7, 8 and 9 of the documents.  
[https://static.goanywhere.com/guides/ga\\_installation\\_guide.pdf](https://static.goanywhere.com/guides/ga_installation_guide.pdf)

### **3.2 Installing GoAnywhere MFT**

Once all the prerequisites are completed, follow the below steps to install GoAnywhere MFT 6.8:

#### **Installing GoAnywhere on Windows**

GoAnywhere can be installed onto a Windows server for enterprise usage. GoAnywhere can also be installed onto Windows desktops or laptops, which is useful for individual development and testing purposes. Both 32-bit and 64-bit versions of Windows are supported.

The TOE has been evaluated on the following host platforms:

- Windows Server 2016 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)

Perform the following steps to install the GoAnywhere product onto a Windows machine.

1. Login to the target Windows system as an administrator.
2. Download the GoAnywhere installer .EXE file from the GoAnywhere Customer Portal at [my.goanywhere.com](http://my.goanywhere.com).
3. Execute the downloaded .EXE file and follow the prompts on the screens.
4. If you did not choose to start the GoAnywhere application server within the installer, then you can manually start this server by following these instructions:
  - a. Go to Control Panel > Administrative tools > Services.
  - b. In the Services window, right-click on GoAnywhere and select Start.
  - c. Within seconds after starting GoAnywhere, its status should be updated to "Started". If not, please contact Fortra technical support.
5. The installation and startup of GoAnywhere is complete. Now you should proceed to the Initial Configuration instructions.

#### **Installing GoAnywhere on Linux**

GoAnywhere MFT is a powerful automation tool that is capable of executing native Linux commands and programs, as well as file actions such as read, write, and delete. It is recommended to designate a non-root user on the system that will be used to install and run the GoAnywhere application. This user will be the owner of all files created during installation as well as files written to the file system during use.

The TOE has been evaluated on the following host platforms:

- CentOS 7 on ESXi 6.7 with Intel Xeon E5-4620v4 (Broadwell)

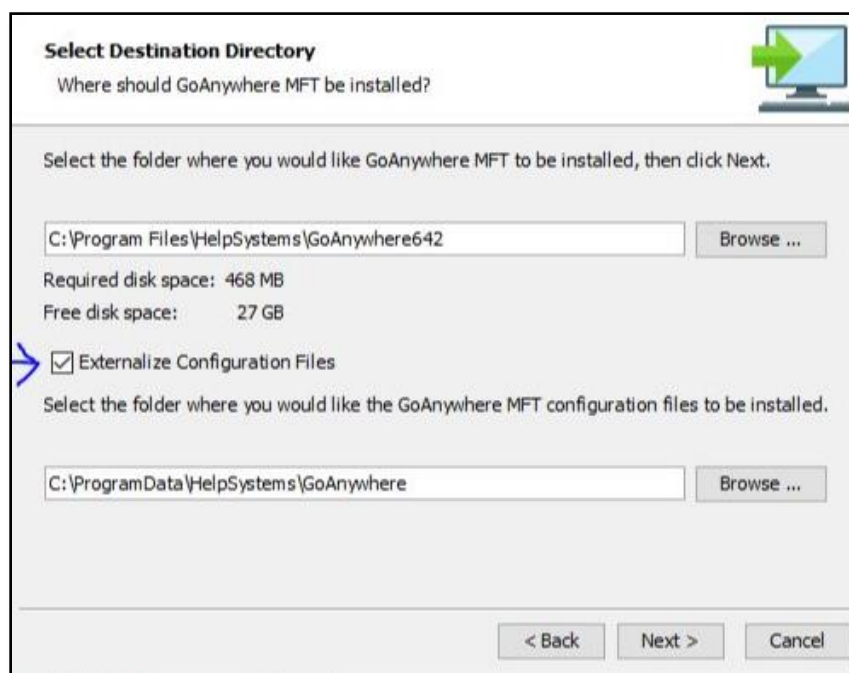
Perform the following steps to install the GoAnywhere RPM onto a Linux system.

1. Create or designate a user with root or sudo privileges on the system that will be used to install and run the GoAnywhere application. This user will be the owner of all files created during installation as well as files written to the file system during use.
2. Login to the target Linux system as the user designated in step 1.
3. Download the GoAnywhere Linux RPM installer file from the URL provided by Fortra.
4. Execute the downloaded installer file by running `sudo yum install <rpm_file>` and follow the prompts.
5. Start GoAnywhere by following these instructions: a.
  - a. Open a Terminal window.
  - b. Start GoAnywhere by executing the following shell script:`sudo service goanywhere-mft start`
6. The installation and startup of GoAnywhere is complete. Now you should proceed to the Initial Configuration instructions.

Note: To meet the Common Criteria requirements, the application installation package is distributed in the format of the platform-supported package manager i.e., the application installer package for Windows platform is distributed in “.EXE” format and “.RPM” format for the CentOS7 (Linux) platform.

Execute the command `sudo rpm -i installer_filename.rpm` to install GoAnywhere on the CentOS7 platform and run the executable file on Windows Platform.

For Common criteria, during the installation process, it must be made sure to externalize Configuration files by enabling the “Externalize Configuration Files”.



The TOE on Windows Platform is composed of Java and native code. The native code implements stack-based buffer overflow protections, being compiled with the /GS flag on Windows. All Java objects are

strictly typed with explicit sizes, so it is not possible to overflow a buffer in Java code. The TOE on Linux Platform is composed of Java code. All Java objects are strictly typed with explicit sizes, so it is not possible to overflow a buffer in Java code.

## **4 Platform Security and Cryptography**

### **4.1 Initial Configurations**

Follow the instructions below to access the software, request a license key, create an administrator account.

1. To access the GoAnywhere Administrator using a secure HTTPS connection, open your browser and type the URL of `https://[hostname]: [port number]` where [hostname] is the host name or IP address of GoAnywhere and [port number] is the port number of the GoAnywhere Administrator. The default HTTPS port for the Administrator is 8001. Example: `https://myserver:8001`.
2. The License Server page appears. Click the Get License button and follow the on-screen prompts to license the server.
3. Once the server is licensed, you are prompted to create an administrator account for GoAnywhere. This account is assigned all administrator roles with access rights to the entire GoAnywhere application. After this account is created, other Admin User accounts can be created from the Users > Admin Users page by clicking on the Add Admin User icon.
4. Specify a Username, password, define the roles, domain and save the configuration.
5. The GoAnywhere Administrator dashboard is displayed.

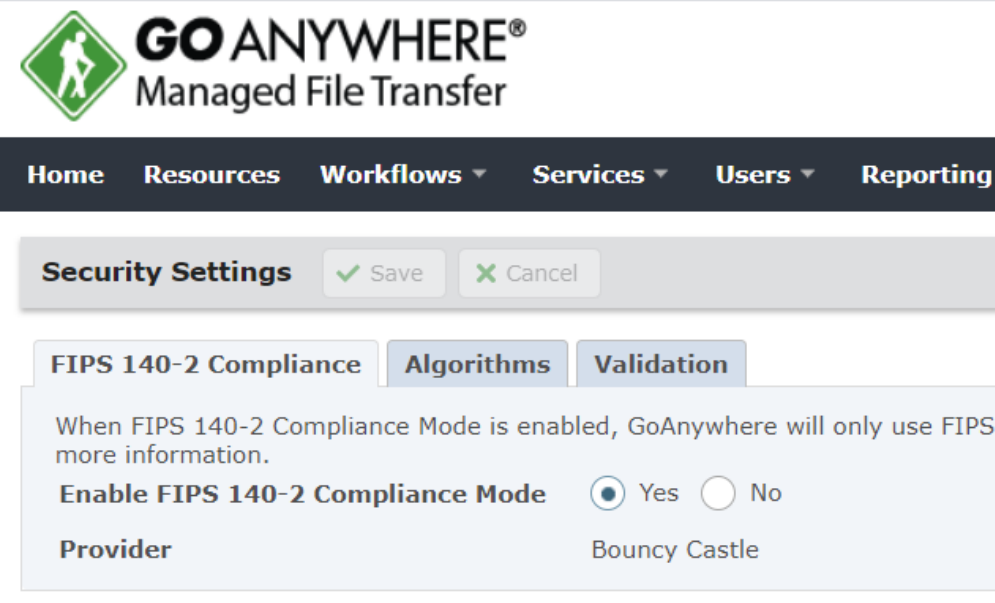
### **4.2 Enabling FIPS 140-2 mode**

The TOE utilizes the GoAnywhere MFT Bouncy Castle FIPS Java API cryptographic library version 1.0.2. This library implements all the cryptographic algorithms required for SSH and TLS, drawing entropy from the platform RBG. The Federal Information Processing Standard (FIPS) is a set of requirements used by the US Federal Government and agencies/companies that do business with them to ensure all sensitive data is encrypted with approved encryption algorithms (ciphers). GoAnywhere provides a FIPS 140-2 Compliance Mode and when enabled, it only permits the use of FIPS 140-2 compliant ciphers for encrypting the data. The Administrator must ensure that the FIPS 140-2 mode is always enabled to implement only evaluated encryption algorithms as other cryptographic engines were not evaluated or tested during the Common Criteria evaluation of the product. The GoAnywhere MFT automatically generates and performs RSAES-PKCS1-v1\_5 key transport with RSA 2048-bit, 3072-bit, and 4096-bit keys that are used for digital signature and key agreement services in TLS when the application is set to FIPS 140-2 mode. The TOE automatically generates and performs Elliptic Curve Diffie-Hellman with curves ECDSA P-256, P-384 which are used for

key agreement services in TLS in FIPS 140-2 Compliance mode. There is no specific configuration required for generating these keys apart from selecting the common criteria compliant cipher-suites that must be supported by the application as seen in SSL/TLS Configuration.

Follow the instructions below to enable FIPS 140-2 Compliance Mode:

1. Log in as an Admin User with the Security Officer role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select System, and then click the Security Settings from the drop-down menu.
3. In the Security Settings page, Enable the FIPS 140-2 Compliance Mode by clicking the radio button Yes in the FIPS 140-2 Compliance section.
4. Click the ✓ Save button.
5. Restart GoAnywhere for the change to take effect.



**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows ▾ Services ▾ Users ▾ Reporting

**Security Settings** ✓ Save ✗ Cancel

**FIPS 140-2 Compliance** Algorithms Validation

When FIPS 140-2 Compliance Mode is enabled, GoAnywhere will only use FIPS more information.

**Enable FIPS 140-2 Compliance Mode** ☒ Yes ☐ No

**Provider** Bouncy Castle

### 4.3 Certificate Validation

Certificate validation is used to specify checks to enforce when validating certificates.

1. Go to Systems->Security Settings->Certificate Validation page

2. Check the boxes for CA Basic Constraints, Date Validation, Extended Key Usage Validation and CRL for Client, Server, and Email certificates and enable them.
3. Provide the URL information after enabling the Certification Revocation Check. The application reaches the URL configured to fetch the CRLs from an external entity. The application reaches the URL every 5 minutes by default to fetch the CRLs. This refresh interval is configurable in minutes.

**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows Services Users Reporting Encryption System Help

Security Settings

FIPS 140-2 Compliance Algorithms Validation

**Certificate Validation**  
Specify checks to enforce when validating client, server, and email certificates.

**CA Basic Constraints Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Date Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Extended Key Usage Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Certificate Revocation Lists (CRL)** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Refresh Interval**  Minutes

**URLs** [Add URL](#)

URL
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/RootCA.crl"/>
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/ICA1.crl"/>
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/ICA2.crl"/>

#### 4.4 Hostname Verification

For Common Criteria configuration, the Hostname Verification is set to yes by clicking the radio button. When set to "Yes", the hostname for all SSL/TLS connections must match any Subject Alternative Name (SAN) IP/DNS entries or the Subject Common Name (CN) on the server's certificate. With Strict Hostname Verification, wildcards "\*" may only comprise the entire left-most portion of a SAN DNS entry or CN (\*.example.com).

1. Go to Systems -> Security Settings -> Validation section.
2. For Common Criteria, the Hostname verification must be set to YES by clicking the radio button.
3. Click the ☒ Save button.
4. Restart GoAnywhere for the change to take effect.

**Security Settings**

**FIPS 140-2 Compliance** **Algorithms** **Validation**

**Certificate Validation**  
Specify checks to enforce when validating client, server, and email certificates.

**CA Basic Constraints Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Date Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Extended Key Usage Validation** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Certificate Revocation Lists (CRL)** ☒ Client Certificates ☒ Server Certificates ☒ Email Certificates

**Refresh Interval**  Minutes

**URLs** [Add URL](#)

URL
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/RootCA.crl"/>
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/ICA1.crl"/>
<input checked="" type="checkbox"/> <input type="text" value="http://10.1.3.51/ICA2.crl"/>

**Hostname Verification**  
Specify whether or not to strictly enforce hostname verification. If set to "Yes", the hostname for all SSL/TLS connections must only comprise the entire left-most portion of a SAN DNS entry or CN (\*.example.com). If set to "No", protocol specific hostname

**Strict Hostname Verification** ☒ Yes ☐ No

## 4.5 SSL/TLS configuration

The GoAnywhere MFT uses TLS encryption to communicate securely with various IT environment devices. The algorithms settings are useful in setting the TLS protocol versions and cipher suites to be used globally by the application. The GoAnywhere MFT Application automatically configures references identifiers based on the FQDN or IP address configured used to specify the TLS server. The Application compares the FQDN, or IP address configured to specify the TLS server against the identifiers in the presented X.509 certificates for certificate validation.

After the FIPS 140-2 Compliance Mode is enabled on the TOE, the Administrator must manually configure the allowed Protocols (TLSv1.2) and allowed cipher suites in the Algorithms section. The configured Algorithm settings are applicable for FTPS, HTTPS, AS2, SSL, SMTPS, GoFast, and Agent communications, as well as database connections and User authentication over SSL (LDAPS). The following steps must be followed to configure the Algorithms.

1. Go to System->Security Settings->Algorithms
2. Under Protocols drag and drop the protocol version of TLS to be used by the GoAnywhere MFT. For Common criteria, select TLSv1.2 as an allowed version.
3. Under Cipher suites drag and drop the cipher suites for TLS communication that should be allowed by the GoAnywhere MFT.



The following cipher suites must be supported by the TOE.

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246,  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,  
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,  
TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288,  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289,  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289,  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289

4. Click the ✓ Save button.
5. Restart GoAnywhere for the change to take effect.

**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows Services Users Reporting Encryption System Help

Security Settings

FIPS 140-2 Compliance Algorithms Validation

Specify the SSL/TLS protocol versions and cipher suites to allow globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider.

Protocols	Disabled	Allowed
	TLSv1 TLSv1.1	TLSv1.2

Cipher Suites	Disabled	Allowed
	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CCM TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CCM TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CCM	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

## 5 Setting up secure communication

### 5.1 Database Configuration


The GoAnywhere MFT is configured to communicate with an external Database server over TLSv1.2.

For Common Criteria, the database of GoAnywhere needs to be externalized and must be communicating with the MFT in TLS encrypted format. To change the database from the default derby database The GoAnywhere database can utilize (connect to) one of the following database types for storing its configuration settings and application data:

- DB2/400 (IBM i) - V5R4 and later
- Derby (Embedded) - 10.12.1.1 (preferred Derby database version)
- Derby (Network) - 10.12.1.1 (preferred Derby database version)
- Microsoft SQL Server - SQL Server 2008 and later
- MySQL - 5.1 and later
- MariaDB versions 5.5 or 10.0 and later
- Oracle - 10g and later
- PostgreSQL 9.6 and later

However, it is recommended to utilize the JDBC Driver for MySQL/MariaDB Database for storing the TOE's configuration settings as this was the only database type that was tested as a part of the Common Criteria Evaluation. It is not recommended to leverage other database types as no assurance to the correct operation of these features is provided.

For configuring the MFT to communicate via TLS with an external MySQL database follow the steps below:

1. Upload Certificate authority (CA) certificate that signs the database server's certificate under Encryption-> Key Management Services.
2. The MFT Application comes with a default Key vault "System" for storing the trusted CA certificates, as well as the private keys/certificates used in the server modules.
3. Click on the  Gear icon next to System Key vault and select Manage Certificates.
4. Click on Import and choose the CA file, file format, and Name of the certificate to import the self-signed CA certificate to the Application Trust store.
5. Go to System-> Database configuration and select Switch Database tab

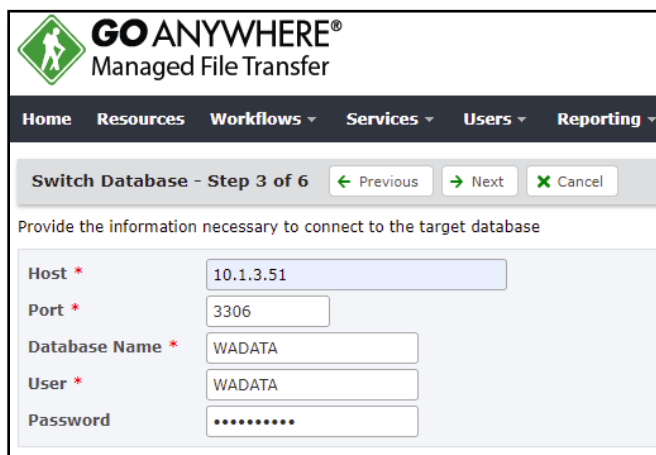
6. Select a Database Server from the list of available database server types and then click Next



**Database Server \***

- ☐ Derby (Embedded)
- ☐ Derby (Network)
- ☒ MySQL/MariaDB
- ☐ Microsoft SQL Server
- ☐ Oracle
- ☐ DB2/400 (IBM i)
- ☐ PostgreSQL

7. Based on the selected database server, some prerequisites may need to be completed before proceeding. For MySQL server follow these steps
- Create a new database (also called schema) by running the statement `CREATE DATABASE GADATA CHARSET=UTF8`
  - Create a new database user by running the statement `CREATE USER GADATA IDENTIFIED BY 'password'`
  - Grant full permissions to the new database created in step 1 to the user created in step 2, by running the statement `GRANT ALL ON GADATA.* TO 'GADATA'`
  - Upload the server certificate signed by the MFT trusted certificate authority and its corresponding key to the MySQL database.
8. Based on the selected database server, provide the requested connection information. The connection credentials are verified after clicking the Next button. If there are connection errors, a description of the connection error is displayed on the page. Connection errors must be corrected before continuing. The example below shows a connection being made to a DB2 database.



**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows Services Users Reporting

**Switch Database - Step 3 of 6** Previous Next Cancel

Provide the information necessary to connect to the target database

Host \* 10.1.3.51

Port \* 3306

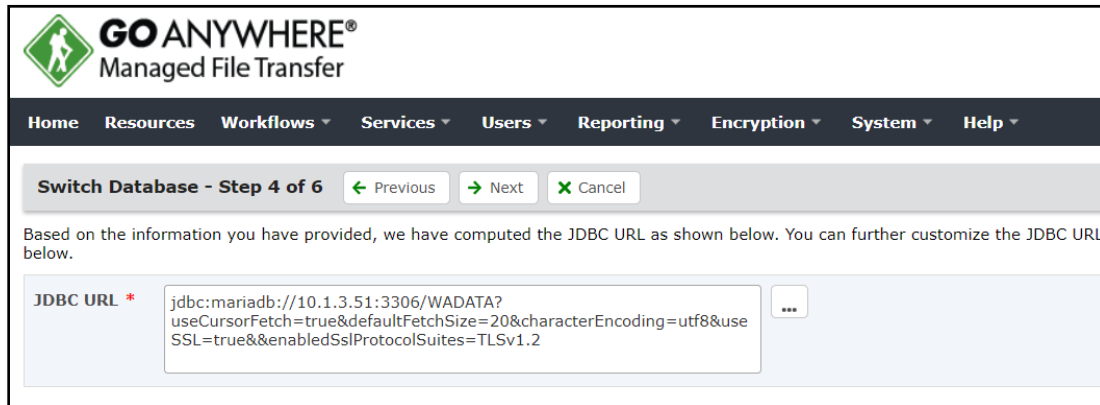
Database Name \* WADATA

User \* WADATA

Password .....

9. Based on the database server selected and the connection information from Step 8, a JDBC URL is automatically composed. If needed, the JDBC URL can be modified on this page or through the JDBC URL Wizard by clicking the ... button. For Common Criteria in addition to the default URL, the parameters `useSSL=true` and `enabledSslProtocolSuites=TLSv1.2` must be added to specify the version of SSL that the MFT leverage to communicate with the external database in an encrypted format.

Reference Identifier: For the TLS connections with the database server, the reference identifier is configured in the JDBC URL as shown below.



**GO ANYWHERE®**  
Managed File Transfer

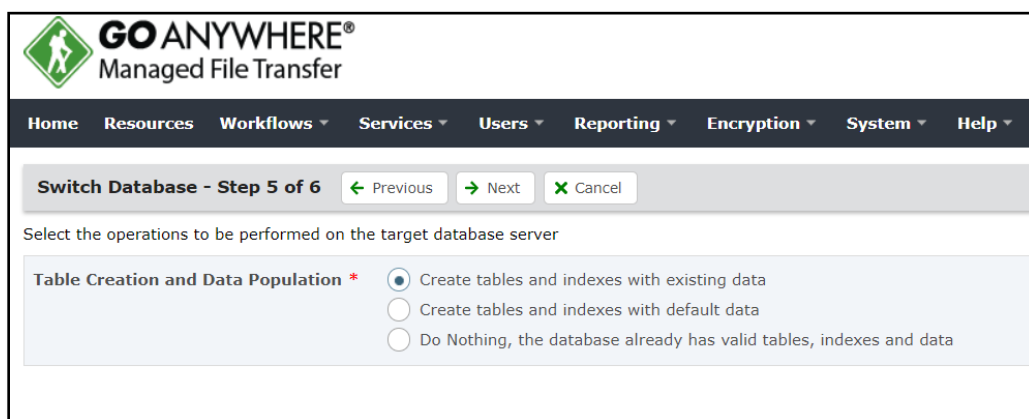
Home Resources Workflows Services Users Reporting Encryption System Help

Switch Database - Step 4 of 6 Previous Next Cancel

Based on the information you have provided, we have computed the JDBC URL as shown below. You can further customize the JDBC URL below.

JDBC URL \* jdbc:mariadb://10.1.3.51:3306/WADATA?useCursorFetch=true&defaultFetchSize=20&characterEncoding=utf8&useSSL=true&enabledSslProtocolSuites=TLSv1.2 ...

10. With the connection configuration complete, select how the Switch Database process will migrate the database. The first option will make a copy of the existing GoAnywhere data to the new database. The second option will create a new database configured for use by GoAnywhere with the default data, just as it was when it was first installed. The third option will not configure the new database or populate any data.



**GO ANYWHERE®**  
Managed File Transfer

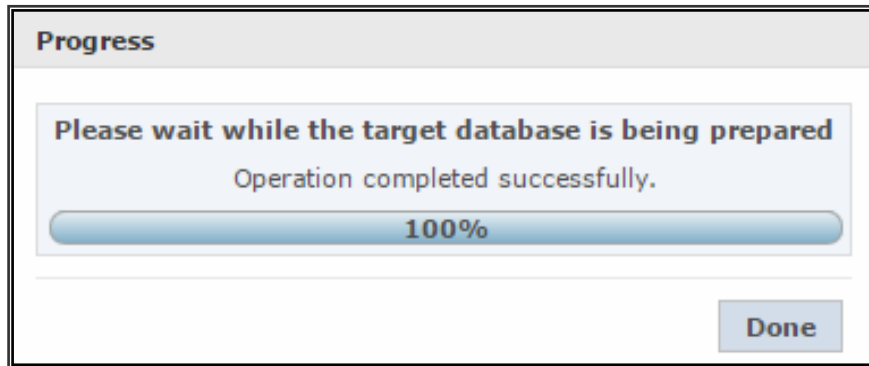
Home Resources Workflows Services Users Reporting Encryption System Help

Switch Database - Step 5 of 6 Previous Next Cancel

Select the operations to be performed on the target database server

Table Creation and Data Population \* ☒ Create tables and indexes with existing data  
☐ Create tables and indexes with default data  
☐ Do Nothing, the database already has valid tables, indexes and data

11. When all the required information for the database change is specified, those settings will then be displayed for review. If you wish to change any of these settings, then click the Previous button to return to the page where the change is needed. If the settings are correct, click Finish to perform the database switch. The Switch Database process will stop any services and close all open connections. After clicking the Finish button, a Progress box opens to display the switch



database progress. When complete, click the Done button.

### Custom Provider for the Database Password

GoAnywhere MFT can be configured to call a custom JAR file that will provide the password for connecting to the database. This allows a separate security management process to handle the storage and decryption of the database password. These steps must be followed whenever the Database configuration is initiated. For Common Criteria evaluated configuration, the following steps must be configured to allow a separate security management process to handle the storage and decryption of the database password.

#### Step 1 – Create your JAR file.

You will need to create a JAR file that integrates with your security management process. The dependencies you will work with and the logic for integration is up to you. The only requirement from GoAnywhere MFT is that the JAR has an entry point that meets this definition:

- The implementation class must be public and cannot be abstract.
- The implementation method must be a public static method that does not take any arguments and returns a String.
  - This String will be used as the password when connecting to the database.

#### Step 2 – Make the JAR available to GoAnywhere MFT.

Once you have your JAR file created, place it in the userdata/lib folder. If your JAR has any dependent JAR files, place them in the userdata/lib folder as well. The name of the files does not matter as long as it ends with '.jar' and is not in a sub-folder of userdata/lib.

#### Step 3 – Configure GoAnywhere MFT to use the custom provider.

Edit the config/database.xml file and make the following changes:

- Remove these lines
  - `<entry key="password">...</entry>`

- <entry key="passwordIsEncrypted">false</entry>
- Add these lines
  - <entry key="implementationClass">com.example.PasswordProvider</entry>
  - <entry key="implementationMethod">getPassword</entry>

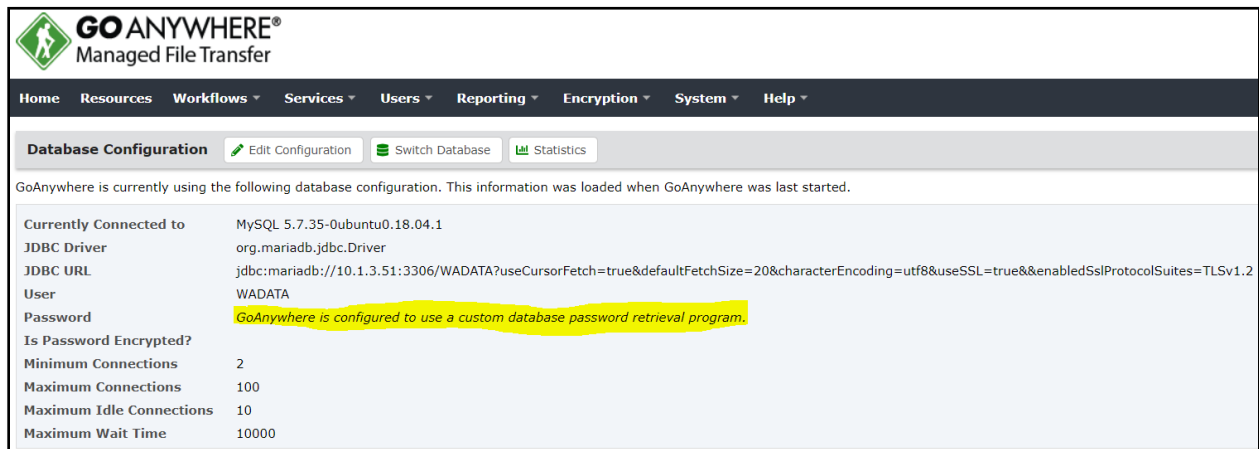
The implementationClass and implementationMethod will need to match the entry point of your JAR file.

#### Step 4 – Restart GoAnywhere MFT

A restart of GoAnywhere MFT is required for these changes to take effect.

#### NOTE - Clustering

If running in a clustered environment, then steps 2 through 4 must be implemented on each node of the cluster.



**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows Services Users Reporting Encryption System Help

Database Configuration Edit Configuration Switch Database Statistics

GoAnywhere is currently using the following database configuration. This information was loaded when GoAnywhere was last started.

Currently Connected to	MySQL 5.7.35-0ubuntu0.18.04.1
JDBC Driver	org.mariadb.jdbc.Driver
JDBC URL	jdbc:mariadb://10.1.1.3.51:3306/WADATA?useCursorFetch=true&defaultFetchSize=20&characterEncoding=utf8&useSSL=true&enabledSslProtocolSuites=TLSv1.2
User	WADATA
Password	GoAnywhere is configured to use a custom database password retrieval program.
Is Password Encrypted?	
Minimum Connections	2
Maximum Connections	100
Maximum Idle Connections	10
Maximum Wait Time	10000

12. Database migration can be verified by ensuring the system->Database configuration has the default Database as desired Target Database.

13. TLS connection can be verified using packet capture tools on DB server.

## 5.2 Authentication Server Configuration

The GoAnywhere MFT is configured to communicate with an external authentication server over TLSv1.2.

LDAP, or Lightweight Directory Access Protocol, is used to query directory services for information, such as authentication credentials. GoAnywhere MFT can be configured to use LDAP as a login method, allowing administrators to manage users while maintaining high security standards more easily.

In GoAnywhere, a Group is used to control permissions and features granted to users who belong to the group. For example, a Development Group could be limited to create Project Workflows or administrate Secure Forms. A Support Group could be limited to reviewing the system or project logs.

A GoAnywhere LDAP Managed Group only allows users to be a member of that group if the user belongs to an LDAP group that has been defined in an LDAP Server Login Method. Once the LDAP Server Login Method

has been created, you will then create LDAP Managed Groups that provide the users permissions to the application.


In GoAnywhere, a Group is used to control permissions and features granted to users who belong to the group. For example, a Development Group could be limited to create Project Workflows or administrate Secure Forms. A Support Group could be limited to reviewing the system or project logs. A GoAnywhere LDAP Managed Group only allows users to be a member of that group if the user belongs to an LDAP group that has been defined in an LDAP Server Login Method. Once the LDAP Server Login Method has been created, you will then create LDAP Managed Groups that provide the users permissions to the application.

Follow the instructions below to configure an LDAP Server Login Method in GoAnywhere MFT:

1. Log in as an Admin User with the Security Officer role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role
2. From the main menu bar, select Users, and then click the Login Methods link.
3. To add a new LDAP server, in the Login Methods page, click the Add Login Method link in the page toolbar.
4. In the Select Login Method Type page, select LDAP Managed. Choose your LDAP Server Type and the User Type that will be managed by this LDAP Login Method.

The Server tab contains the fields used to establish a connection to the LDAP server. Define the following fields:

- Name - A unique name for the LDAP Login Method.
- Primary Host - The host name or IP address of the LDAP server.
- Port - The port number for the LDAP server.
- Use SSL - Enable this option to use SSL for secure transmission with the LDAP server. This must be enabled as a part of the Common Criteria Evaluated configuration.
- Implicit SSL - When enabled, GoAnywhere will trust any certificate from the LDAP server. When not enabled, the certificate will be validated using the Key Management System. This must not be enabled as a part of the Common Criteria Evaluated configuration.
- User - An LDAP trusted user ID for performing searches within the LDAP server.
- Password - The password for the trusted user ID. To update an existing password, click the Change Password link and specify a new password.
- Base DN - The Base DN within the LDAP server restricts where GoAnywhere will find users and groups in the directory tree.
- Object Class Attribute - The name of the attribute that holds the class value for a LDAP entry. Object class determines the type of object, such as a user, organizational unit, or domain.
- Distinguished Name Attribute - The name of the attribute that stores the unique identifier for a LDAP entry.


**GO ANYWHERE®**  
 Managed File Transfer

Home Resources Workflows Services Users Reporting Encryption System Help

Edit LDAP Server Save Cancel

Server Admin Users Advanced User Group Membership

**Name \***

**Description**

512 Characters Remaining

**User Type**

**Primary Host \***

**Alternate Host**

**Port \***

**Use SSL** ☒

**Implicit SSL** ☐

**User \***

**Password \*** [Change Password](#)

**Base DN \***

**Object Class Attribute \***

**Distinguished Name Attribute \***

The Web Users or Admin Users tab controls how users in the LDAP server are integrated with the Users in GoAnywhere.

**Synchronization**

☒ Synchronization Enabled  
 Users from the LDAP server will be automatically copied into GoAnywhere accounts during the synchronization process.

Run every  minutes

**User Authentication**

☒ Create User Automatically During Login  
 If the User account does not exist in GoAnywhere during login, their account will automatically be created if the supplied user and password is valid on the LDAP server.

☒ Update User Info  
 When the User logs in, GoAnywhere will update their account information with the latest details retrieved from the LDAP server.

**User Groups**

☒ Enforce Group Membership  
 The User can login only if they belong to a Group in GoAnywhere that is associated with this Login Method.

**Template**

If the User is created automatically from this LDAP server, specify the template to use.




The Advanced tab allows you to set log levels and server timeout settings. You can view these logs in the Logs > Audit Logs > Server Logs page in GoAnywhere

Log Level	Summary ▼
Connection Timeout	60 ▲▼
Read Timeout	300 ▲▼
Search Timeout	0 ▲▼

The User tab allows you to configure the LDAP schema settings for finding users. GoAnywhere populates these fields using default attributes based on the type of LDAP server selected.

Define the following fields:

- Object Class - The object class name for a user. You can view the default objectClass and other attribute values in the LDAP entry. In this example, the default objectClass of user objects is inetOrgPerson.
- Username - The attribute for a username.

**GO ANYWHERE®**  
Managed File Transfer

Environment: [Click Here](#)  
Logged in as: **acumensec**

[Change Password](#) | [API Keys](#) | [Log Out](#)

Home Resources Workflows ▾ Services ▾ Users ▾ Reporting ▾ Encryption ▾

Add LDAP Server ✓ Save ✗ Cancel ?

Server Admin Users **Advanced** User Group Membership

**Filter**

Object Class \*

Object Filter

**Attribute Mappings**

User Name \*

Email

Membership

- The Group tab allows you to configure LDAP settings for finding groups. GoAnywhere populates these fields using default attributes based on the type of LDAP server selected. Define the following fields:
  - Object Class - The object class name for a group.
  - Name - The attribute for the group name.

**Add LDAP Server**   ?

Server Web Users Advanced User **Group** Membership

**Filter**

Object Class \*

Object Filter

**Attribute Mappings**

Name \*

Membership

The Membership tab allows you to specify if membership is defined by the Group or User. If 'Group defines membership' is selected, membership will be defined by the Membership attribute specified on the Group tab. If 'User defines membership' is selected, membership will be defined by the Membership attribute specified on the User tab.

Server Web Users Advanced User Group **Membership**

Membership Source

Include Nested Groups ☒

## Linking GoAnywhere User Groups to an LDAP Login Method

When you create a new Admin User Group or Web User Group in GoAnywhere, you will be prompted to select which type of group will be used to manage user membership. Choose the LDAP Managed Group, and then specify the following:

- Login Method – Select the LDAP Login Method you just configured.
- LDAP Group – GoAnywhere will use the LDAP configuration and return a list of LDAP Groups that could be found using the settings in the LDAP Group tab. Select the desired group from the available groups in the selected LDAP server.

For Web Users, give the group a name and description and specify the Services, Resources, Folder, and Form permissions for the group in the respective General, Folders and Forms tabs.

For Admin Users, give the group a name and a description, and specify the Roles, Members, and Domains that will be available to the administrators that belong to this group

The group members will be synced with the LDAP Group chosen previously. Repeat this process for every group you would like to create using this login method.

The screenshot displays two side-by-side configuration windows in GoAnywhere. The left window, titled 'Select Web User Group Type', has buttons for 'Continue' and 'Cancel'. It instructs the user to select a group type: 'GoAnywhere Group' (unselected) or 'LDAP Managed Group' (selected). Below, the 'Login Method' is set to 'ApacheDS' and the 'LDAP Group' is set to 'support'. The right window, titled 'Add Web User Group', has buttons for 'Save' and 'Cancel'. It features four tabs: 'General', 'Members', 'Folders', and 'Forms'. The 'General' tab is active, showing a 'Group Name' field with 'Support', a 'Domain' field with 'Default', and a 'Description' text area. Below these are checkboxes for 'Protocols' (AS2, FTP, FTPS, GoFast, HTTPS, SFTP), 'GoDrive', 'Secure Folders', 'Secure Forms', 'Send Secure Mail', 'Send Invitations', and 'View Activity Report'. The 'Protocols' section shows 'FTP', 'FTPS', 'GoFast', and 'HTTPS' checked, while 'AS2' and 'SFTP' are unchecked. 'GoDrive' is also unchecked. 'Secure Folders', 'Secure Forms', and 'Send Secure Mail' are checked. 'Send Invitations' and 'View Activity Report' are unchecked.

## 5.3 Admin Server Configuration

The GoAnywhere MFT is configured as an Administration server in order to allow the users access the Application UI over TLSv1.2.

The Admin Server page provides the ability to modify the GoAnywhere Admin Server connection and listener. To manage the Admin Server, log in as an Admin User with the Product Administrator role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

- If the admin server port is mapped to an IPv6 address, follow the steps below to change the mapping to IPv4


#### Windows:

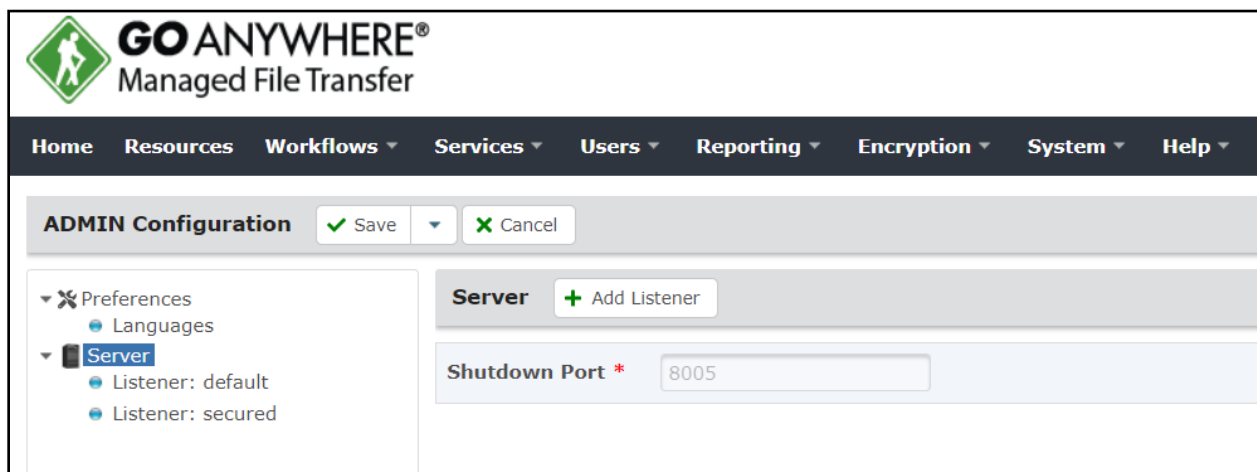
1. Navigate to the GoAnywhere's [Installation directory] \tomcat\bin folder and run GoAnywherew.exe as administrator.
2. NOTE: This may also be GoAnywhereServicesw.exe if MFT was previously a GoAnywhere Services instance.
3. In the menu that appears, click into the Java tab and insert the following at the end of the Java Options field: -Djava.net.preferIPv4Stack=true
4. Click Apply and OK.
5. Restart the GoAnywhere service for the changes to take effect.

#### Linux:

1. Navigate to the GoAnywhere's [Installation directory]/tomcat/bin folder and edit the start\_tomcat.sh file.
2. Add '-Djava.net.preferIPv4Stack=true' to the JAVA\_OPTS section at the beginning of the file.  
NOTE: The option line should look like this:  
JAVA\_OPTS='-Xmx1024m -XX:MaxPermSize=256m -Djava.awt.headless=true  
-Djava.net.preferIPv4Stack=true -XX: -UseVMInterruptibleIO'
3. Save the file.
4. Restart the GoAnywhere service/subsystem for the changes to take effect.
  - Make sure the firewall settings are appropriately set on the OS Platform for the admin server to become accessible from the client

#### Server:

Navigate to System > Admin Server. Click on the  edit icon next to Administrator and the following page will be displayed. Click on the server icon.



**GO ANYWHERE®**  
Managed File Transfer

Home Resources Workflows Services Users Reporting Encryption System Help

**ADMIN Configuration** ✓ Save ✗ Cancel

**Preferences**

- Languages
- Server**
  - Listener: default
  - Listener: secured

**Server** + Add Listener

**Shutdown Port \***

- Shutdown Port

The TCP/IP port number on which GoAnywhere waits for a shutdown command. This connection must be initiated from the same server or computer that is running this instance of GoAnywhere.

- Admin Configuration Options
  - Add Listener to a server by clicking the **+** Add Listener button in the page toolbar
  - View or Modify a Listener by clicking the Listener name in the left column

- Listener

Listeners will monitor for IP traffic and route traffic based on configured settings. The default listener settings supplied in GoAnywhere should meet the needs for most installations. The Admin Listeners are used to specify connection timeouts, SSL settings, and ports to access GoAnywhere through an Internet browse. To delete a Listener entry, click the Delete button in the page toolbar. For the Administrator listeners, it is recommended to disable them instead of removing them.

- Name

Providing an identifiable name for the listener helps identify it in the Configuration Outline list.

- Port

Listeners monitor specific port numbers. Set the port number that the listener will monitor. 8001 is the default port used by the listener for secure connections.

- Protocol

Sets the protocol to handle incoming traffic. The default value is HTTP/1.1.

This is the IP address of the server hosting the port to which you are listening. If available, you can also select it from the drop-down list.

- Enable Lookups

When lookups are enabled, the server will search for and report servers by their DNS name. If lookups are not used only the IP address is returned.

- Disable Upload Timeout

Lengthy uploads may decrease server performance or be the result of an error. Select whether uploads are subject to timeouts

- Compression

File compression may increase transfer rates, but lower processing speeds. By default, compression is set to On and will compress only text data. If set to Off, no compression is used on files and if compression is set to Force, compression is used for all files.

- No Compression User Agents

This option allows a user with the System Administrator role, in certain instances, to specify the header data of a browser for which files will never be compressed.

- Connection Timeout

The number of seconds this connection will remain open before closing if no requests are sent. The default is 60 seconds.

- Maximum Threads

The maximum number of threads created by the connection for request processing on this Listener. This determines the maximum number of simultaneous requests that can be handled. The default is 200 threads.

- Minimum Spare Threads

This is the number of threads that will be created when this listener is first started. The default is four (4) threads

- Server Header

When a User makes a connection to GoAnywhere via HTTP or HTTPS, the server replies to the client with the name and version of the server in one of the headers. The Server Header field can be used to customize the server information that is returned. This setting should only be specified when attempting to hide the identity of the server for security purposes.

- Proxy Name

The Proxy Name attribute can be used when GoAnywhere is run behind a proxy server. This attribute modifies the value returned to web applications that call the `request.getServerName()` method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned would reflect the server name on which the connection from the proxy server was received, rather than the server name to whom the client directed the original request.

- Proxy Port

The Proxy Port attribute can be used when GoAnywhere is run behind a proxy server. This attribute modifies the value returned to web applications that call the `request.getServerPort()` method, which is often used to construct absolute URLs for redirects. Without configuring this attribute, the value returned

would reflect the server port on which the connection from the proxy server was received, rather than the server port to whom the client directed the original request

## SSL Tab

The screenshot shows the 'ADMIN Configuration' window for 'GO ANYWHERE Managed File Transfer'. The 'Listener' configuration is selected, and the 'SSL' tab is active. The configuration includes fields for 'SSL Enabled' (set to 'Yes'), 'SSL Protocol' (set to 'TLS'), 'Enabled SSL Protocols' (set to 'TLSv1.2'), 'Key Store Algorithm', 'Trust Store Algorithm' (set to 'X509'), 'Client Authentication' (set to 'Required'), and 'Enabled Cipher Suites'. The 'Enabled Cipher Suites' section shows a list of available cipher suites on the left and a list of selected cipher suites on the right. The 'Certificate Location' is set to 'System Key Vault', and the 'Key Name' is 'https\_server'. There is a 'Key Password' field with a 'Change Password' link. An 'Export Head Certificate' button is also present.

Available	Selected
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM_8	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- SSL Enabled

From the drop-down list, select the appropriate option:

- Yes - A Secure Socket Layer is used to secure transmissions.

- SSL Protocol

Specify the appropriate option:

- TLS - A new version of SSL, Transport Layer Security will be used to secure the transmission (default).

- Enabled SSL Protocols

Specify a comma separated list of SSL/TLS protocol versions to allow. To enable TLS 1.2 only, specify TLSv1.2.

- Client Authentication

This determines how the client will authenticate with the server.

For Non mutual connection

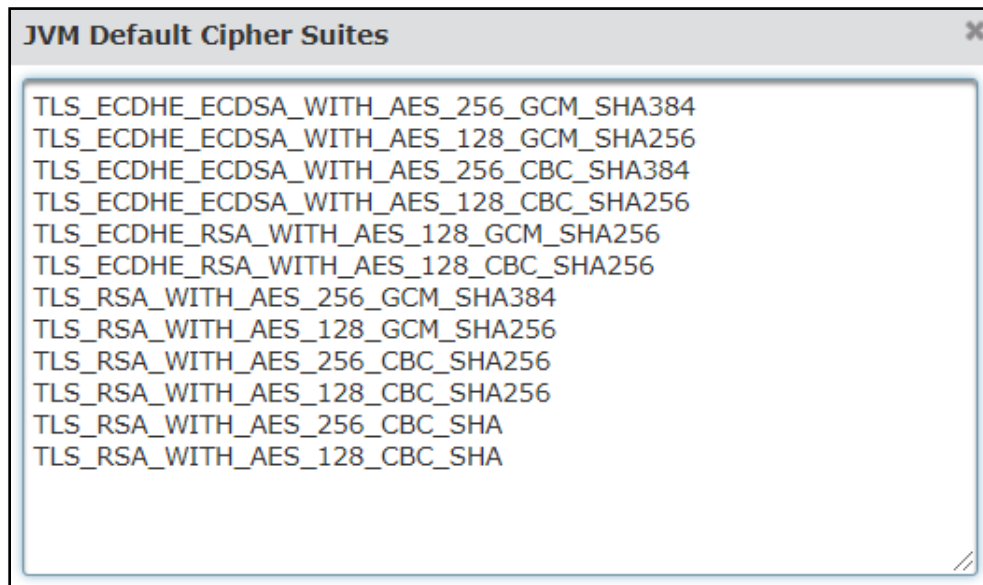
None - The SSL connection runs without checking certificates and the User is authenticated with a password. If any of the information being transmitted requires a certificate, the connection will fail

For mutual authentication:

Required - The SSL connection will not connect or authenticate a User unless a valid certificate is available. It must be ensured that the Client authentication is set to Required for TLS mutual authentication as a part of the Common Criteria evaluated configuration.

- Enabled Cipher Suites

By default, the JVM Default Cipher Suites are used when no cipher suites are selected. Click the JVM Cipher Suites link to view a list of the default cipher suites. This list of default cipher suites corresponds to the cipher suites being claimed as a part of the evaluation. However, the cipher suites supported by the TOE are configurable.




Although encrypted, the cipher suite automatically selected by the connection may not be the most secure. This list allows you to limit which ciphers are used. Follow the instructions below to select the following Cipher Suites that must be supported by the TOE.

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246,
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288,
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288,
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289,



TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 as defined in RFC 5289,  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289,  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5289,  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289

1. In the left column, click to select (highlight) the Cipher Suites to use. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Cipher Suites are selected, click the  arrow between the group boxes to move the Cipher Suites from left to right

- **Certificate Location**

The location of the private key used to identify the server and location where incoming client certificates are trusted. Select System Key Vault. Key Vaults are stored in the remote database that is configured as a part of the Database Configuration.

#### System Key Vault

The private key and associated certificates are stored in the Key Management System. All certificates within the KMS are used to establish trust for user authentication.

- **Key Name**

Select the private certificate from the System Key Vault. This key is used to identify the server's identity.

- **Key Password**

The password for accessing the certificate. This is only required if the password is not stored in the Key Vault. To update an existing Password, click the Change Password link and specify a new password.

As a part of the evaluated configuration, it must be made sure that the GoAnywhere MFT stores certificates and keys in an external database. After configuring the remote Database as required for the evaluated configuration, select the System key Vault for certificate location. The server certificate and key are imported to the KMS as a key pair. Type the name or click the Browse icon to browse for the file.

## 5.4 HTTPS Server Configuration

The GoAnywhere MFT is configured to communicate with an external HTTPS server over TLSv1.2 for securely exchanging files.

GoAnywhere can connect to HTTPS servers for securely exchanging files over encrypted SSL connections. When defining a HTTPS server resource in GoAnywhere, you need to indicate the HTTPS connection

properties such as the host name (or IP address), and optionally the SSL certificates, user, password and proxy information.

#### Basic Tab

<b>Name *</b>	<input type="text" value="Healthcare HTTPS Server"/>
<b>Description</b>	<input type="text"/>
<b>Host *</b>	<input type="text" value="www.example.com"/>

- Name

A user-defined name which identifies the HTTPS server. This name should be descriptive enough so users can quickly identify this HTTPS server when prompted to choose from a list (for example, "Bank HTTPS Server"). The name cannot exceed 50 characters.

- Description

A short paragraph that describes the HTTPS server. The description is optional.

- Host

The host name or IP address of the HTTPS server.

- Connection Tab

<b>Port</b>	<input type="text" value="443"/>
<b>User</b>	<input type="text"/>
<b>Password</b>	<input type="text"/>
<b>Connection Timeout</b>	<input type="text" value="60"/>
<b>Read Timeout</b>	<input type="text" value="30"/>
<b>SSL Context Protocol</b>	<input type="text"/>

- Port

The port number to use for connecting to the HTTPS server. If this field is left blank, then the default port number of 443 will be used. This must be configured to the port number on which the server accepts HTTPS connections.

- User

The username (login name) to use for connecting to the HTTPS server. This is only needed if the HTTPS server requires that the HTTPS client be authenticated using either the BASIC or DIGEST authentication schemes.

- Password

The password to use for connecting to the HTTPS server. This is only needed if the HTTPS server requires that the HTTPS client be authenticated using either the BASIC or DIGEST authentication schemes. To update an existing Password, click the Change Password link and specify a new password. If Allow Viewing of Resource Passwords is enabled on the Admin Security Settings page, an additional Password Recovery icon password recovery option is available.

- Connection Timeout

The maximum amount of time, in seconds, to wait when trying to establish a connection to the HTTPS server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default value of 60 seconds will be used.

- Read Timeout

The maximum amount of time, in seconds, to wait for a (read) response from the HTTPS server. A timeout value of 0 (zero) is interpreted as an infinite wait time. If the field is left blank, then the default infinite value of 0 (zero) will be used.

- SSL Context Protocol

Specify a protocol to use when creating the SSL Context. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). Valid values could include TLSv1.2.

- Certificates Tab

Specify the server certificate options for validating the HTTPS server's identity and the client certificate options for validating the client's identity.

### Key Vault Keys

The integrated Key Management Systems allows administrators to create Key Vaults in GoAnywhere that are used to create and store certificates, SSH keys. By Default, Key Vaults are stored in the GoAnywhere database. For Common Criteria, the database of GoAnywhere needs to be externalized and must be communicating with the MFT in TLS encrypted format. After externalizing the database, the default System Key Vault and newly created key vaults are stored in the remote database.

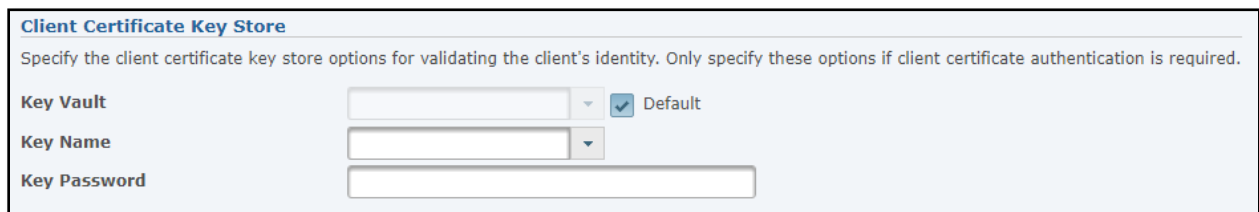
- Server Certificate Key Store

File Based Keys or Key Vault Keys are used by the application to create and manage certificates, SSH keys. The File Based keys are stored on file systems, as opposed to the Key Management System (Key Vaults) that stores keys in the configured database. For common criteria, Key Management System will be used for validating the HTTPS server's identity and File Based Key settings will not be visible as it is disabled at the Domain level.

The certificates located in Key Vaults associated to the Domain and in the System Key Vault will be used to validate that the HTTPS server is trusted.

- Client Certificate Key Store

The Client Certificate Key Store settings are only required when the server requires that HTTPS client connections be authenticated with a certificate.



The screenshot shows a configuration form titled "Client Certificate Key Store". Below the title is a descriptive text: "Specify the client certificate key store options for validating the client's identity. Only specify these options if client certificate authentication is required." The form contains three fields: "Key Vault" with a dropdown menu and a checked "Default" checkbox, "Key Name" with a dropdown menu, and "Key Password" with a text input field.

- Key Vault

Specify the Key Vault containing the client certificates and private keys. This is required only when the HTTPS server requires that HTTPS clients are authenticated with a certificate. The Domain's default Key Vault will be used unless a different Key Vault is selected.

- Key Name

Select the desired certificate from a drop-down list of certificates located in the Key Vault.


- Key Password

The password protecting the secret (private) key portion of the selected key pair. This field is not required if the password is already stored along with the key in the Key Vault. To update an existing Password, click the Change Password link and specify a new password. If Allow Viewing of Resource Passwords is enabled on the Admin Security Settings page, an additional Password Recovery icon password recovery option is available.

## 5.5 SFTP Server Configuration

The GoAnywhere MFT is configured as an SFTP server in order to allow users to transmit large files over SSH 2.0.

The SFTP Service Configuration page provides the configuration options for the SFTP Service.

1. To manage the SFTP Service, log in as an Admin User with the Product Administrator role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select Services and then click the Service Manager link.
3. Click the  Action icon next to the SFTP Service, and then click Edit.

- General

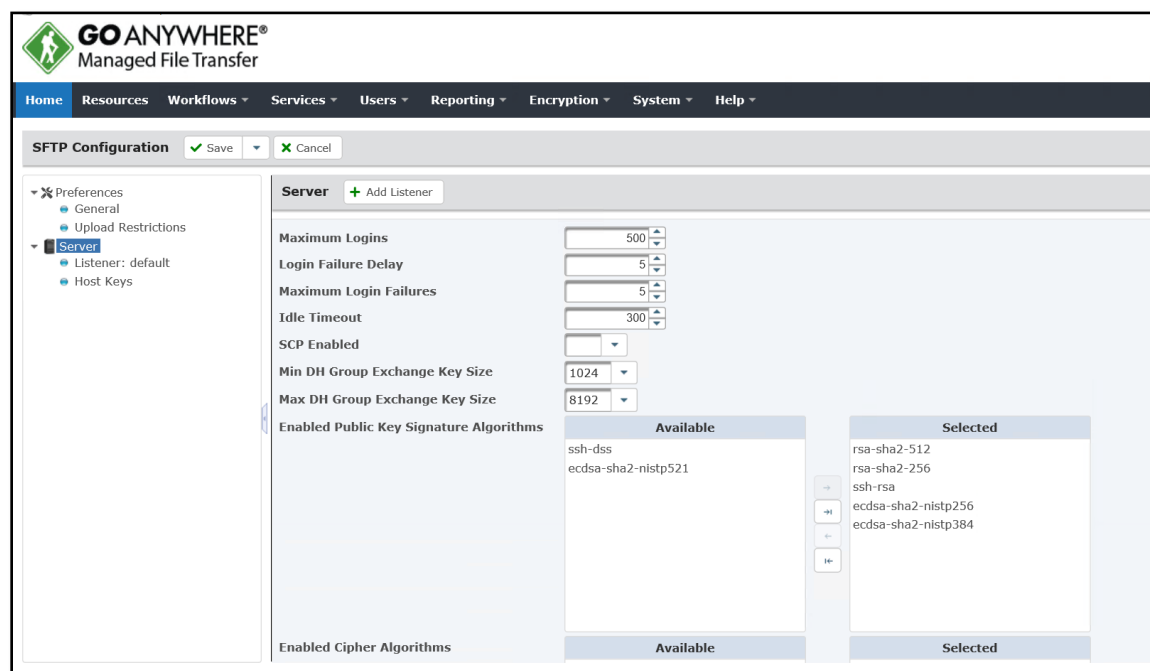
**Automatically Start Service** ☒ Yes ☐ No

### Automatically Start Service

Specify whether you would like to start the SFTP service automatically when GoAnywhere starts.

- Server

- a. Enabled Public Key Algorithms




The screenshot shows the GoAnywhere Managed File Transfer interface. The top navigation bar includes Home, Resources, Workflows, Services, Users, Reporting, Encryption, System, and Help. The main content area is titled 'SFTP Configuration' and includes 'Save' and 'Cancel' buttons. On the left, a sidebar shows 'Preferences' with 'General', 'Upload Restrictions', and 'Server' (selected). The 'Server' section has a '+ Add Listener' button. The configuration fields include: Maximum Logins (500), Login Failure Delay (5), Maximum Login Failures (5), Idle Timeout (300), SCP Enabled (checkbox), Min DH Group Exchange Key Size (1024), and Max DH Group Exchange Key Size (8192). The 'Enabled Public Key Signature Algorithms' section features two columns: 'Available' (listing ssh-dss and ecdsa-sha2-nistp521) and 'Selected' (listing rsa-sha2-512, rsa-sha2-256, ssh-rsa, ecdsa-sha2-nistp256, and ecdsa-sha2-nistp384). Below this is the 'Enabled Cipher Algorithms' section with 'Available' and 'Selected' columns.


The Public key Algorithms in the left column are available, the ones in the right column are enabled. By default, all public key algorithms are enabled to provide the most options between different clients and

servers. This list allows you to limit which public key algorithms are used. Follow the instructions below to select the following Public key Algorithms that are compliant as per the evaluation: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, and ecdsa-sha2-nistp384.

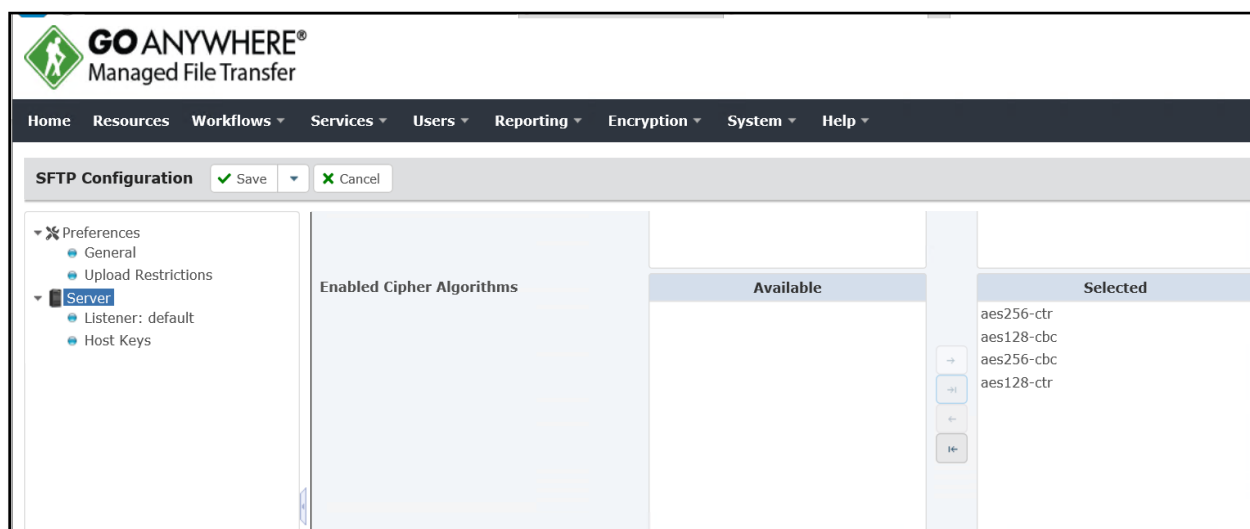
Perform the following steps to enable Public key Algorithms:

1. On the left side of the page, click to select (highlight) the Public key Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Public key Algorithms are selected, click the  arrow between the group boxes to move the algorithms from left to right.

Perform the following steps to disable Public key Algorithms:

1. On the right side of the page, click to select (highlight) the Public key Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Public key algorithms are selected, click the  arrow between the group boxes to move the algorithms from right to left.


#### b. Enabled Cipher Algorithms




The Cipher Algorithms in the left column are available, the ones in the right column are enabled. By default, all Cipher Suites are enabled to provide the most options between different clients and servers. Although encrypted, the cipher suite automatically selected by the connection may not be the most secure. This list allows you to limit which ciphers are used. Follow the instructions below to select the following Cipher Algorithms that are compliant as per the evaluation: aes128-ctr, aes256-ctr, aes128-cbc, and aes256-cbc.

Perform the following steps to enable Cipher Algorithms:

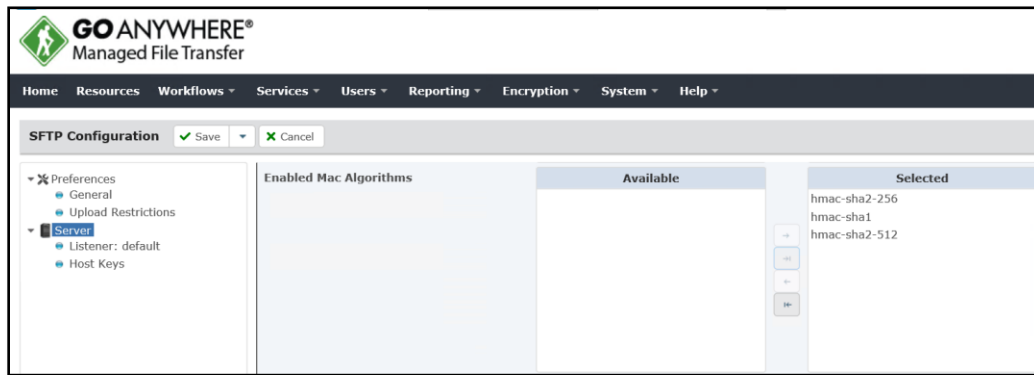
3. On the left side of the page, click to select (highlight) the Cipher Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.

- When the desired Cipher Algorithms are selected, click the  arrow between the group boxes to move the algorithms from left to right.

Perform the following steps to disable Cipher Algorithms:


- On the right side of the page, click to select (highlight) the Cipher Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
- When the desired Cipher Algorithms are selected, click the  arrow between the group boxes to move the algorithms from right to left.

### c. Enabled Mac Algorithms




The SSH transport layer handles algorithm negotiation between the server and client over TCP/IP. Negotiation begins when the SSH client and server send each other textual information that identifies their SSH version. If they both agree that the versions are compatible, the client and server exchange lists that specify the algorithms that they support for key exchange, encryption, and data integrity via a message authentication code (MAC). These lists are protected by their own encryption algorithms. The Mac Algorithms in the left column are available, the ones in the right column are enabled. Follow the instructions below to select the following MAC Algorithms that are compliant as per the evaluation: hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

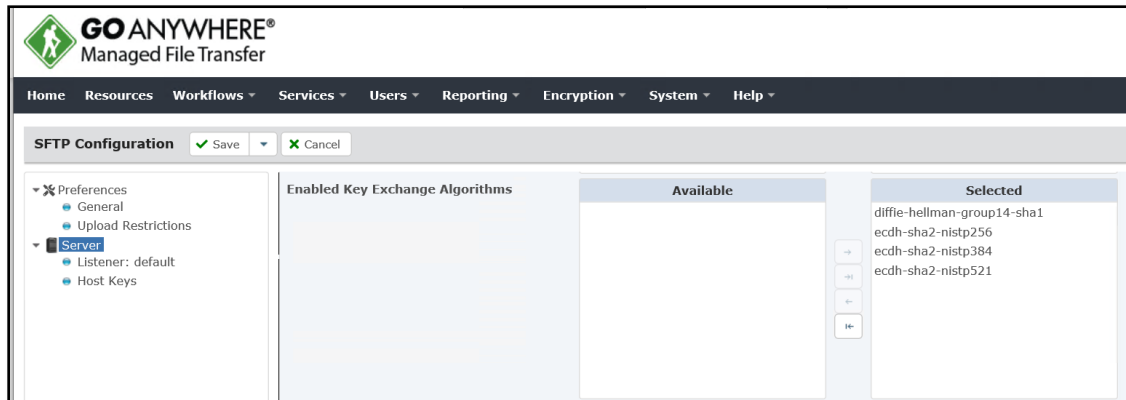
Perform the following steps to enable Mac Algorithms:

- On the left side of the page, click to select (highlight) the Mac Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
- When the desired Mac Algorithms are selected, click the  Right arrow between the group boxes to move the algorithms from left to right.

Perform the following steps to disable Mac Algorithms:


- On the right side of the page, click to select (highlight) the Mac Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
- When the desired Mac Algorithms are selected, click the  Left arrow between the group boxes to move the algorithms from right to left.

#### d. Enabled Key Exchange Algorithms




The Diffie-Hellman Key exchange algorithms to use between the server and client. The Key Exchange Algorithms in the left column are available, the ones in the right column are enabled. This list allows you to limit which Key Exchange Algorithms are used. Follow the instructions below to select the following Key Exchange Algorithms that are compliant as per the evaluation: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.

Perform the following steps to enable Key Exchange Algorithms:

1. On the left side of the page, click to select (highlight) the Key Exchange Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Key Exchange Algorithms are selected, click the  arrow between the group boxes to move the algorithms from left to right.

Perform the following steps to disable Key Exchange Algorithms:

1. On the right side of the page, click to select (highlight) the Key Exchange Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Key Exchange Algorithms are selected, click the  Left arrow between the group boxes to move the algorithms from right to left.

- Listener

The screenshot shows the 'Listener' configuration form. The form has five fields: Name (default), Port (22), Local Address (10.1.4.1), Domain (Sales), and Authentication Types Allowed (Either).

- Local Address



This is the IP address of the server hosting the port to which GoAnywhere is Listening. If available, you can also select it from the drop-down list.

- Domain

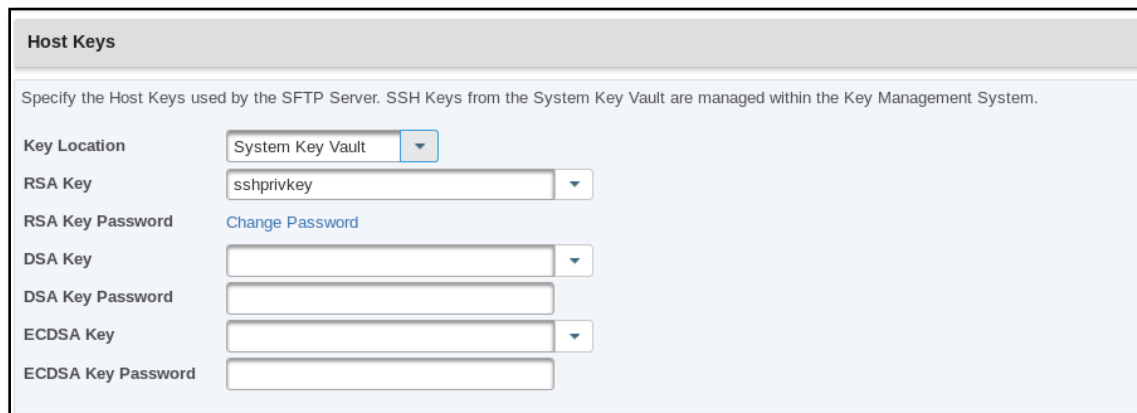
A Domain can be specified to restrict this listener to only allow Web Users in that Domain. When left blank, any Web User can login regardless of which Domain they belong to.

- Authentication Types Allowed

Indicates which authentication types are allowed on this listener - Password, Public Key, or Either. If left blank, the default value is Either. When a Web User attempts to authenticate, this setting, as well as the authentication type specified on the individual Web User account, are verified.

- Host Keys

RSA and ECDSA keys are used to identify the server. RSA keys and ECDSA keys are typically limited to use for the evaluation.



The screenshot shows the 'Host Keys' configuration window. At the top, it says 'Specify the Host Keys used by the SFTP Server. SSH Keys from the System Key Vault are managed within the Key Management System.' Below this, there are several fields: 'Key Location' is a dropdown menu set to 'System Key Vault'; 'RSA Key' is a dropdown menu set to 'sshprivkey'; 'RSA Key Password' is a text field with a 'Change Password' link next to it; 'DSA Key' is a dropdown menu; 'DSA Key Password' is a text field; 'ECDSA Key' is a dropdown menu; and 'ECDSA Key Password' is a text field.

- Key Location

RSA and ECDSA keys can be selected from the System Key Vault, or another location on the network. Select the location where your keys are stored. For common criteria, the DSA keys must not be added or selected as a part of the evaluation.

- RSA Key

Select an RSA key from the System Key Vault.

- RSA Key Password

The password to access the RSA key. The password is only required if it is not stored along with the key in the Key Vault.

- ECDSA Key

Select an ECDSA key from the System Key Vault. When using ECDSA keys, the Public Key Signature Algorithm must match the key type and bit size of the Host Key. For example, when creating an ECDSA Host Key with a 256 bit key size, the `ecdsa-sha2-nistp256` public key algorithm should be enabled.

- ECDSA Key Password

The password to access the ECDSA key. The password is only required if it is not stored along with the key in the Key Vault.

## 5.6 SFTP Client Configuration

The GoAnywhere MFT is configured to communicate with an external SFTP server to perform file transfers over SSH 2.0.

GoAnywhere can connect to SSH Servers for performing SFTP (SSH File Transfer Protocol) file transfers, SCP (Secure Copy) file transfers and for running SSH remote commands. When defining an SSH Server resource in GoAnywhere, you need to indicate the connection properties such as the host name (or IP address) and User ID. You can specify a password, SSH private key or both for authentication.

SFTP Servers can be configured as Resources in GoAnywhere and then specified as file repositories for Web User virtual folder locations. Projects in GoAnywhere can also connect to SFTP resources to upload, download, and manage documents by using qualified file paths (using the resource name) within various Tasks.

### Basic Tab

<b>Name *</b>	<input type="text" value="SFTP Server"/>
<b>Domain</b>	<input type="text" value="Default"/>
<b>Description</b>	<input type="text"/>
<b>Host *</b>	<input type="text" value="10.1.4.1"/>
<b>Port</b>	<input type="text"/>
<b>User</b>	<input type="text" value="kharris"/>
<b>Password</b>	<input type="password" value="....."/>
<b>Key Location</b>	<input type="text" value="Key Vault"/> ▼
<b>Key Vault</b>	<input type="text"/> ▼ <input checked="" type="checkbox"/> Default
<b>Key Name</b>	<input type="text" value="Trading Partner"/> ▼
<b>Key Password</b>	<input type="password" value="....."/>

- Name

A user-defined name which identifies the server. This name should be descriptive enough so a user can quickly identify this server when prompted to choose from a list (for example, Bank SFTP Server). The name cannot exceed 50 characters.

- Description

A short paragraph that describes the server. The description is optional.

- Host

The host name or IP address of the server.


- Port

The port number to use for connecting to the server. If left blank, the default port number is 22.

- User

The username (login name) to use for connecting to the server. A username is only required if using password authentication or both password and SSH private key authentication

- Password

The password to use for connecting to the server. A password is only required if using password authentication or both password and SSH private key authentication. To update an existing Password, click the Change Password link and specify a new password. If Allow Viewing of Resource Passwords is enabled on the Admin Security Settings page, an additional  password recovery option is available.

- Key Location

Select to use Key Vault keys for this resource. The evaluated configuration uses Key Vaults.


- Key Vault

The Key Vault containing the private ssh keys used for client authentication. The Domain's default Key Vault will be used unless a different Key Vault is selected.


- Key Name

Select the desired key from a drop-down list of keys located in the Key Vault.

- Key Password

The password protecting the secret (private) key portion of the selected ssh key. This field is not required if the password is already stored along with the key in the Key Vault. To update an existing Password, click the Change Password link and specify a new password. If Allow Viewing of Resource Passwords is enabled on the Admin Security Settings page, an additional  password recovery option is available.

## Connection Tab

Host Key	<input type="text"/>
Timeout	<input type="text" value="180"/>
Connection Retry Attempts	<input type="text" value="10"/>
Connection Retry Interval	<input type="text" value="5"/>
Initial Remote Directory	<input type="text" value="/inbound/reports"/>
Throttle Bandwidth	<input type="text"/> 

- Host Key

The fingerprint of the server's public key, which will be used to authenticate the server. If a fingerprint is not specified, then the server will be treated as trusted.

- Timeout

The number of seconds to wait when attempting to connect to the server. A timeout will occur if the connection cannot be established in the specified amount of time. If this field is left blank, the default timeout value is 120.

- Connection Retry Attempts

The number of times to retry the connection if it cannot be established. This setting is used for both the initial connection and any reconnect attempts due to lost connections. If left blank, then no retries will be attempted.

- Connection Retry Interval

The number of seconds to wait between each connection retry attempt.

## Algorithms Tab


The options on the Algorithms tab allow customization of the supported algorithms for each SSH server resource. The entries in the left column are the available algorithms and the entries in the right column are the selected algorithms. By selecting one or more algorithms, only those will be used during the communication. If no algorithms are selected for a section, the defaults for that section will be used. Refer to the Default Algorithms section below for the list of defaults.

During the handshake process, the selected options are negotiated with the server, starting with the entry at the top of the list. The first cipher, mac, key exchange, and compression algorithms to match an algorithm supported by the server will be used for the connection. If your company prefers certain algorithms over others, use the arrow buttons to move that cipher to the Selected column and to set the order with the most preferred algorithm at the top. Press the CTRL key while clicking to select multiple entries. In FIPS 140-2 Compliance Mode, the cipher, Mac and Key exchange algorithms are not configurable, and the application uses only the claimed algorithms as per Common criteria requirements and no other algorithms.


### a. Enabled Authentication Methods

Follow the instructions below to select the following Authentication methods that are compliant as per the evaluation: public-key and password-based authentication.

Perform the following steps to enable specific Authentication methods:

1. On the left side of the page, click to select (highlight) the Authentication method(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Authentication methods are selected, click the  arrow between the group boxes to move the algorithms from left to right.


Perform the following steps to disable Authentication methods:

1. On the right side of the page, click to select (highlight) the Authentication method(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Authentication methods (gssapi-with-mic and gssapi-with-mic) are selected, click the  arrow between the group boxes to move the algorithms from right to left.


### b. Enabled Host Key Signature Algorithms

Follow the instructions below to select the following Host key Signature Algorithms that are compliant as per the evaluation: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, and ecdsa-sha2-nistp384.

Perform the following steps to enable Host key Signature Algorithms:

1. On the left side of the page, click to select (highlight) the Host key Signature Algorithm(s) to enable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Host key Signature Algorithms are selected, click the  arrow between the group boxes to move the algorithms from left to right.

Perform the following steps to disable Host key Signature Algorithms:

1. On the right side of the page, click to select (highlight) the Host key Signature Algorithm(s) to disable. Multiple entries can be selected by pressing the Ctrl or Shift key while clicking the mouse.
2. When the desired Host key Signature algorithms are selected, click the  arrow between the group boxes to move the algorithms from right to left.

#### c. Enabled Cipher Algorithms

The FIPS 140-2 Compliance Mode must enabled as a part of the evaluated configuration. In FIPS 140-2 Compliance Mode, the GoAnywhere MFT only supports the following encryption algorithms and no other algorithms: aes128-ctr, aes256-ctr, aes128-cbc, and aes256-cbc.

#### d. Enabled MAC or Data integrity algorithms.

The FIPS 140-2 Compliance Mode must enabled as a part of the evaluated configuration. In FIPS 140-2 Compliance Mode, the GoAnywhere MFT only supports the following data integrity algorithms and no other algorithms: hmac-sha1, hmac-sha1-96, hmac-sha2-256, and hmac-sha2-512.

#### e. Enabled Key Exchange Algorithms

The FIPS 140-2 Compliance Mode must enabled as a part of the evaluated configuration. In FIPS 140-2 Compliance Mode, the GoAnywhere MFT only supports the following key exchange algorithms and no other algorithms: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.

Specify the authentication options and algorithms to use for this SFTP, SCP, or SSH connection. If no entries are selected within a section below, then the defaults will be used for that section. See the help text for more information.

<b>Authentication</b>	<div>gssapi-with-mic</div> <div>keyboard-interactive</div>	<div>publickey</div> <div>password</div>
	<div>→</div> <div>←</div> <div>↔</div>	
<b>Host Key Signature Algorithms</b>	<div>ssh-dss</div> <div>ecdsa-sha2-nistp521</div>	<div>ssh-rsa</div> <div>rsa-sha2-256</div> <div>rsa-sha2-512</div> <div>ecdsa-sha2-nistp256</div> <div>ecdsa-sha2-nistp384</div>
	<div>→</div> <div>←</div> <div>↔</div>	
<b>Cipher</b>	Ciphers are not configurable. Running in FIPS 140-2 Compliance Mode.	
<b>Mac</b>	Macs are not configurable. Running in FIPS 140-2 Compliance Mode.	
<b>Key Exchange</b>	Key Exchanges are not configurable. Running in FIPS 140-2 Compliance Mode.	

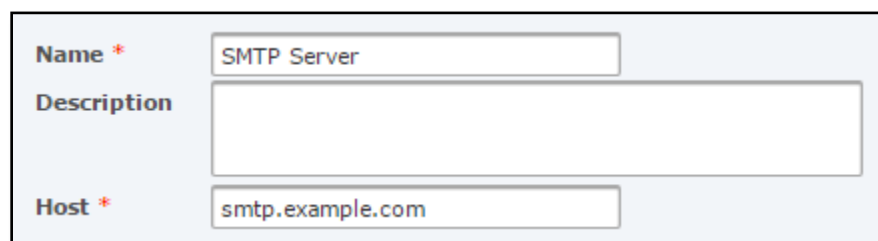
## 5.7 Mail Server Configuration

The GoAnywhere MFT is configured to communicate with an external SMTP server over TLSv1.2.

Go Anywhere can connect to SMTP mail servers for sending email messages. This is especially useful for distributing files as email attachments. When defining a SMTP resource in Go Anywhere, you need to indicate the SMTP connection properties such as the host name (or IP address), and optionally the user and password.

After the FIPS 140-2 Compliance Mode is enabled on the TOE, the Administrator must manually configure the allowed Protocols (TLSv1.2) and allowed cipher suites in the Algorithms section at System -> Security Settings. The configured Algorithm settings are applicable for SMTPS connections. The algorithms settings are useful in setting the TLS protocol versions and cipher suites to be used globally by the application.

### Basic Tab



The screenshot shows a configuration form with three fields: 'Name' with a red asterisk, containing the text 'SMTP Server'; 'Description', which is an empty text area; and 'Host' with a red asterisk, containing the text 'smtp.example.com'.

- Name

A user-defined name which identifies the SMTP server. This name should be descriptive enough so a user can quickly identify this SMTP server when prompted to choose from a list (for example, "Corporate Mail Server"). The name cannot exceed 50 characters.

- Description

A short paragraph that describes the SMTP server. The description is optional.

- Host

The host name or IP address of the SMTP server.

<b>Port</b>	<input type="text" value="465"/>
<b>User</b>	<input type="text" value="testuser1"/>
<b>Password</b>	<input type="password" value="....."/>
<b>Connection Type</b>	<input type="text" value="Implicit SSL"/> ▼
<b>SSL Context Protocol</b>	<input type="text" value="TLS"/>
<b>Enabled SSL Protocols</b>	<input type="text" value="TLSv1.2"/>
<b>Timeout</b>	<input type="text" value="300"/>

- Port

The port number to use for connecting to the SMTP Server. If left blank, the default port is 25.

- User

The username (login name) to use when connecting to the SMTP server. If the user name is left blank, then it is assumed that the SMTP server does not require authentication for its email clients.

- Password

The password to use for connecting to the SMTP server. To update an existing Password, click the Change Password link and specify a new password. If Allow Viewing of Resource Passwords is enabled on the Admin Security Settings page, an additional Password Recovery icon password recovery option is available.

- Connection Type

The following connection type must be used when communicating with the SMTP Server.

- Implicit SSL - The entire connection and transmission is encrypted using SSL.

- SSL Context Protocol

Specify a protocol to use when creating the SSL Context. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). In most cases, the default value (TLS) should just work fine. However, on some IBM JRE implementations the default value would not work if the server you are connecting to does not support TLSv1.

- Enabled SSL Protocols



Specify a comma separated list of SSL/TLS protocol versions to allow. For common criteria enable TLS 1.2 only, specify TLSv1.2.





- Timeout

The maximum amount of time, in seconds, to wait for a response from the SMTP server. A value of 0 (zero) is interpreted as infinite timeout. The default timeout is 300 seconds.

## 5.8 Workflows and Projects

Projects are created in GoAnywhere to automate file transfers and business processes (workflows) for your organization. These Projects can be executed immediately or scheduled to run at future dates and times.



To work with Projects, click Workflows from the main menu, and then click Projects. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

Projects				
<div><div>+ Create a Project</div><div>Q Search Projects</div><div>▼ Import Projects</div><div>▼ Folder</div><div>?</div></div>				
Project Name				
Filter By <input type="text"/>				
<input type="checkbox"/>	Project Name ▾		Description ▾	Modified On ▾
<input type="checkbox"/>	 	Import Case Excel	1/3/19 8:50:14 AM	2/13/19 11:48:29 AM
<input type="checkbox"/>	 	Support Case Reports	11/15/17 12:42:23 PM	1/3/19 9:41:46 AM

### Creating Projects

1. Log in as an Admin User with the Project Designer role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select Workflows, and then click the Projects link.
3. Drill-down to the desired folder to create or edit the Project.
4. Click the **+** Create a Project link in the sub-menu to create a new Project or select a Project from the list to edit it.
5. The GoAnywhere Project Designer page will open.
6. The left-hand column has a list of functions that can be used in these projects
7. Depending on the usage drag and drop the necessary function.
8. For example: For File transfers using SFTP drag and drop the SFTP function under file transfers and then add the Get or Put files function accordingly.

## Validating a Project

1. When done making changes to the Project, click the  Validate link in the sub-menu to validate the syntax of the Project.
2. If the validation was successful, then click the  Save & Finish button to save the Project and return to the folder.
3. Execute the Project.

## 6 Management Functions








The below steps must be followed to perform the functions provided by the Management Console:

### 6.1 Configuring Various System Users:

GoAnywhere implements Roles, Login Methods, Admin Users and Admin Groups to control access to administrative functions in the product.




#### a. Ability to create admin users

To perform administrative functions in GoAnywhere, an Admin User must login with a valid username and password. Admin Users can be added and managed only by an Admin User with the Security Officer role. The passwords for these users can be stored and authenticated within GoAnywhere's database, or can be authenticated against Windows Active Directory (AD), LDAP or an IBM i.

Admin Users <span>+ Add Admin User</span> <span>?</span>					
GoAnywhere can be administered via the users listed below. To access a service (HTTPS/AS2, FTP, FTPS, SFTP and GoFast) you will need to create <a href="#">Web Users</a> .					
<input type="checkbox"/>		User Name	Description	Email	Last Login Date
<input type="checkbox"/>		administrator	Administrator	administrator@example.com	6/1/18 2:02:56 AM
<input type="checkbox"/>		root	Root User (same as administrator)	root@example.com	1/19/19 11:11:43 AM
<input type="checkbox"/>		athomas	GoDrive Manager	athomas@example.com	5/29/18 9:11:01 AM
<input type="checkbox"/>		drobinson	Auditor	drobinson	6/8/18 10:15:02 AM
<input type="checkbox"/>		jsmith	Security Manager	jsmith@example.com	6/8/18 1:47:05 PM
<input type="checkbox"/>		kharris	Security Officer	kharris@example.com	6/14/18 3:58:57 PM
<input type="checkbox"/>		mbarnes	Systems Developer	mbarnes@example.com	9/10/18 4:28:18 PM




## b. Configuring an Admin User

Follow the instructions below to add or edit an Admin User:

1. Log in as an Admin User with the Security Officer role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select Users, and then click the Admin Users link.
3. To add an Admin User, click the **+** Add Admin User link in the page toolbar. Choose the Admin User Template that will apply default Roles, Admin User Groups, and Domain settings for the Admin User, and then click the Continue button.
4. To edit an Admin User, click the  Action icon beside the Admin User you wish to edit, and then click  Edit.
5. Type or edit the Admin User information in the appropriate boxes.
6. If needed, select the individual Roles to be assigned to the Admin User.
7. Assign the Admin User to one or more Groups. The Admin User will adopt the Roles and Domains from any Groups to which it belongs.
8. Assign the Admin User to one or more Domains.
9. Click the  Save button when finished creating or editing the account

## c. Ability to configure Admin User groups



Follow the instructions below to add or edit an Admin User Group:

1. From the main menu bar, select Users, and then click the Admin User Groups link
2. To Add an Admin User Group, click the **+** Add Admin User Group link in the page toolbar
3. To edit an Admin User Group, in the Admin User Groups page, click the  Action icon beside the Admin User Group you wish to edit, and then click  Edit.
4. Type the group information in the appropriate boxes.
5. Select a Group Role, and then use the arrow buttons to move the Group Role to the appropriate column. You can also drag and drop a Group Role from one column to another.
  1. Select a Group Member, and then use the arrow buttons to move the member to the appropriate column. You can also drag and drop a Group Member from one column to another.
  2. Select a Group Domain, and then use the arrow buttons to move the Domain to the appropriate column. You can also drag and drop a Domain from one column to another.
3. Click the  Save button to add the Admin User Group

## d. Ability to configure Admin User Roles

A Role can be assigned to Admin Users and Groups through the Edit Admin User Role page. The Edit Admin User Role page is split in two columns. The Admin Users and Groups not assigned to the role are displayed in the left column. The Admin Users and Groups assigned to the role are displayed in the right column.

Follow the instructions below to edit the Roles for an Admin User or Group:

1. From the main menu bar, select Users, and then click the Admin User Roles link.
2. In the Admin User Roles page, click the  Action icon beside the Role you wish to edit, and then click edit.
3. Assign or remove Admin Users to the appropriate roles. Assign Admin Users or Groups to a Role
4. In the left column, click to select the Admin Users or Groups to assign to the Role. Multiple entries can be selected by pressing the Ctrl or Shift key while selecting Admin Users or Groups.
5. When the desired Admin Users or Groups are selected, click the  icon to move the Admin Users or Groups from left to right.

**Role Name \***

Auditor

**Description**

512 Characters Remaining

**Users**

**Available**

athomas  
jsmith  
kharris  
mbarnes

→

→|

←

|←

**Selected**

**Groups**

**Available**

All Admin Users  
Administration

→

→|




















←

|←



**Selected**

#### e. Admin User Roles Management

To work with roles, log in as an Admin User with the Security Officer role. From the main menu bar, select Users, and then click the Admin User Roles link. To add a new Admin User Role, click the Add icon Add Role button.

Admin User Roles <span>+ Add Role</span> <span>?</span>	
Role Name	Description
 <a href="#">Agent Manager</a>	Admin users in this role can manage Agents
 <a href="#">Auditor</a>	Admin users in this role have View Only Access
 <a href="#">Dashboard Manager</a>	Admin users in this role can manage shared dashboards
 <a href="#">File Manager</a>	Admin users with this role can manage (e.g. download, copy, delete, upload) files on the GoAnywhere server
 <a href="#">Job Manager</a>	Admin users in this role can monitor all active jobs, cancel jobs, pause/resume jobs and view/delete completed jobs
 <a href="#">Key Manager</a>	Admin users with this role can manage various types of encryption keys such as SSH and x509
 <a href="#">Log Viewer</a>	Admin users with this role can access the audit logs
 <a href="#">Partner Manager</a>	Admin users in this role can manage Partners
 <a href="#">Product Administrator</a>	Admin users with this role can perform product administration tasks such as setting the global preferences, applying product updates and fixes, installing/updating product license and more
 <a href="#">Project Designer</a>	Admin users in this role can create, edit and delete projects
 <a href="#">Project Executor</a>	Admin users in this role can execute projects and view jobs they submitted
 <a href="#">Resource Manager</a>	Admin users with this role can manage resources such as FTP, SFTP, Databases, and Network Shares
 <a href="#">Secure Forms Manager</a>	Admin users in this role can manage Secure Forms
 <a href="#">Secure Mail Manager</a>	Admin users with this role can manage packages and Secure Mail settings
 <a href="#">Security Officer</a>	Admin users with this role are allowed to create users, groups and assigning them roles and object authorities
 <a href="#">SLA Manager</a>	Admin users in this role can manage Service Level Agreements
 <a href="#">Trigger Manager</a>	Admin users with this role can manage Triggers and Actions that are executed during events
 <a href="#">Web User Device Manager</a>	Admin users with this role can manage Web User devices
 <a href="#">Web User Manager</a>	Admin users with this role can manage Web Users and Web User Groups

#### f. Remove Admin Users or Groups from a Role:

1. In the right column, click to select the Admin Users or Groups to remove from the role. Multiple entries can be selected by pressing the Ctrl or Shift key while selecting Admin Users or Groups.
2. When the desired Admin Users or Groups are selected, click the  icon to move the Users or Groups from right to left.
3. Click the  Save button to apply the changes.

#### g. Ability to configure identifiers for client authentication

The GoAnywhere MFT allows identifiers to be configured for admin user authentication from a remote web browser.

As shown below the Authentication type can be selected as Certificate with a SHA1 fingerprint of the Client's certificate. The SHA1 Fingerprint of the certificate is used for authentication. Certificates authenticating Admin Users can be verified by the Admin User's username, email address, or both. The Admin User's username is checked against the Subject Distinguished Name (DN) common name (CN) for

a match. The Admin User's email address is checked against a Subject Alternative Name (SAN) Internet Mail Address for a match. If a matching SAN record does not exist, the email address is checked against the Subject Distinguished Name (DN) Email Address. When the user with authentication type set to certificate tries to login to the MFT via a remote web browser, the fingerprint of the certificate being presented by the client is matched against the configured SHA1 Fingerprint on the TOE. Once there is a match, the reference identifier check is performed based on the check boxes selected for SAN/DN Validation. The Admin User's username is checked against the Subject Distinguished Name (DN) common name (CN) for a match when the Username is selected. The Admin User's email address is checked against a Subject Alternative Name (SAN) Internet Mail Address for a match when the email address is selected.

For Common Criteria evaluated configuration, The GoAnywhere MFT must require the DN in the presented certificate to match a DN authorized for the services the client is connecting to. The application then verifies the certificate matches the certificate pinned to the user's account using a SHA-1 hash.

**Edit Admin User** [Save] [Cancel]

User Name \*

Description

Authentication Type

SHA1 Fingerprint \*

SAN/DN Validation ☒ User Name ☐ Email Address

Authentication Alias

Email Address

Office Phone

Mobile Phone

Enabled ☒

Roles

Available	Selected
	Agent Manager
	Auditor
	Dashboard Manager
	File Manager
	Job Manager
	Key Manager
	Log Viewer
	Partner Manager
	Product Administrator
	Project Designer



Groups






Available	Selected


#### h. Ability to create web users:













Web Users are the accounts that can access GoAnywhere for exchanging files using standard protocols. Web Users can be external (for example, Trading Partners) or internal to your company (for example, employees or custom applications). Web Users are managed by an Admin User that has a Web User Manager role. Web Users can be added individually, from an LDAP Managed Login Method, or through an import process that provides the ability to add multiple Web Users based on Web User Templates. A Web User account can also be created through a self-registration process available on the HTTPS Web Client. APIs are also available to create Web Users from your in-house applications




Follow the instructions below to add or edit a Web User:

1. Log in as an Admin User with the Web User Manager role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select Users, and then click the Web Users link.
3. To add a Web User, click the **+** Add Web User link in the page toolbar. Choose the Web User Template that will apply default security settings for the Web User, and then click the Continue button.
4. To edit a Web User, in the Web Users page, click the  Edit icon next to the Web User.
5. Type or edit the Web User information in the appropriate boxes.
6. Click the  Save button when finished.

Web Users <span>+ Add Web User</span> <span>✓ Pending Invitations</span> <span>▼ Import Web Users</span> <span>🔍 View Folder Access</span> <span>?</span>						
Filter By <input type="text" value="User Name"/> <span>More ▼</span> <span>🔄</span> <span>☰</span>						
<input type="checkbox"/>		User Name ▾	First Name ▾	Last Name ▾	Organization ▾	Account Status
<input type="checkbox"/>		anonymous				Disabled
<input type="checkbox"/>		jdoo	John	Doe	HR	Enabled
<input type="checkbox"/>		jsmith	Jenny	Smith	IT	Enabled
<input type="checkbox"/>		kharris	Kathy	Harris	IT	Enabled
<input type="checkbox"/>		tgreen	Tom	Green	HR	Enabled
Showing 1 - 5 of 5 <span>1</span> <span>Rows</span> <span>20</span> <span>Export All</span> <span>Columns</span>						

The following actions are available by selecting the  Actions icon:

- View Web User details by clicking  View.
- View the Web User's File System by clicking  View File System.
- View the Web User's GoDrive by clicking  View File System.
- View the change history for the Web User by clicking  Change History.
- Edit a Web User by clicking  Edit.
- Approve a self-registered Web User by clicking  Approve.
- Reset a Web User's password by clicking  Reset.
- Delete a Web User by clicking .
- Configure the public SSH keys for a Web User by clicking  SSH Keys.
- Move the Web User to a new Domain by clicking  Switch Domain. After selecting the target Domain, you will be given the opportunity to make changes to the Web User before it is saved.
- Promote a Web User's account to another GoAnywhere server by clicking  Promote.
- Export a Web User's account information to an XML file by clicking  Export. The selected Web User(s) are saved in a file named "export-web-users.xml" on your local computer.

- Remove the Time-based One-Time Password authentication secret from this Web User by clicking  Remove TOTP.
- Remove a GoDrive license from this Web User by clicking  Remove License.
- Remove a Secure Mail license from this Web User by clicking  Remove Secure Mail.





## 6.2 Configure Keys and Certificates:

The integrated Key Management Systems allows administrators to create Key Vaults in GoAnywhere that are used to create and store certificates, SSH keys. By Default, Key Vaults are stored in the GoAnywhere database. For Common Criteria, the database of GoAnywhere needs to be externalized and must be communicating with the MFT in TLS encrypted format. After externalizing the database, the default System Key Vault and newly created key vaults are stored in the remote database. GoAnywhere includes two Key Vaults, the System and Default vaults:

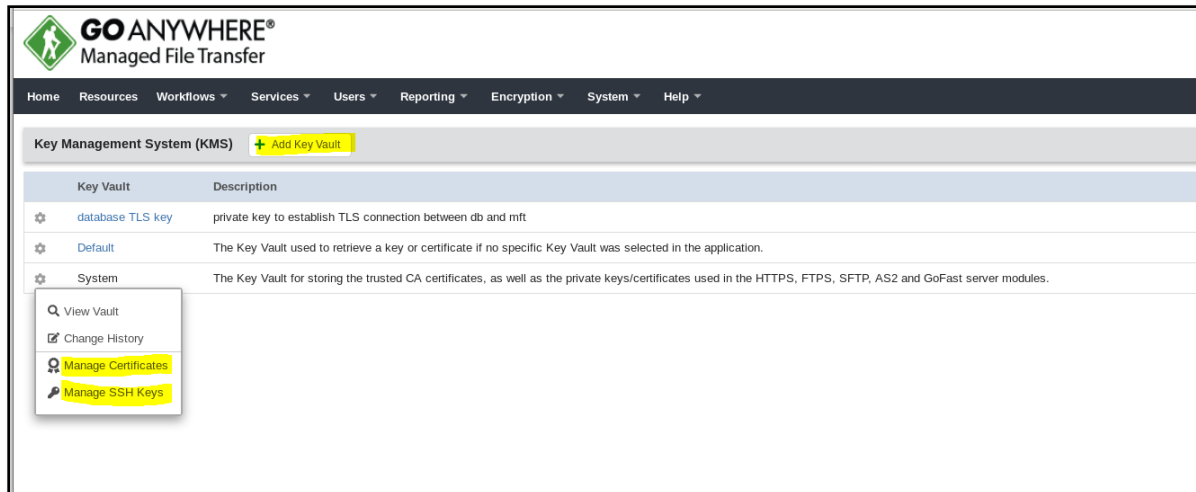
- System - The Key Vault for storing the trusted CA certificates, as well as the private keys/certificates used in the HTTPS, FTPS, SFTP, AS2, and GoFast services.
- Default - A Key Vault used to retrieve keys or certificates for Web User authentication, Resources, and Projects. Additional Key Vaults can be created to organize keys into specific groups, such as Key Vaults that are used by specific Domains.

### 1. Ability to create and manage Key vaults

Follow the instructions below to add or edit a Key Vault:

1. Log in as an Admin User with the Security Officer role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select Encryption, and then click the Key Management System link.
3. To add a Key Vault, click the  Add Key Vault button in the page header.
4. To edit a Key Vault, click the  Action icon next to the desired Key Vault and then click  Edit.
5. Specify or edit the Key Vault information in the appropriate fields.
6. Click the  Save button when finished





## 2. Ability to add certificates

Follow the instructions below to add a new certificate:

1. Log in as an Admin User with the Key Manager role to manage certificates in a Domain's Key Vault. To manage certificates in the System Key Vault, log in as an Admin User with the Product Administrator and Key Manager roles. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select Encryption, and then click the Key Management System link.
3. Click the ⚙️ Action icon next to the desired Key Vault and select 👤 Manage Certificates.
4. In the Certificate Manager page, click + Add Certificate in the page toolbar.
5. On the Add Certificate page, complete the requested information.
6. When complete, click the ✓ Save button to create the certificate

GoAnywhere supports importing DER, PEM, JKS, and PKCS #12 encoded certificates and files that contain multiple certificates. When a file contains multiple certificates, each certificate is imported individually. If a certificate already exists in the Key Vault with the same name, the imported certificate will be renamed automatically by appending a sequential number. Import certificate(s) by following the steps below:

1. Log in as an Admin User with the Key Manager role to manage certificates in a Domain's Key Vault. To manage certificates in the System Key Vault, log in as an Admin User with the Product Administrator and Key Manager roles. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select Encryption, and then click the Key Management System link.

Add Certificate
Save
Cancel
?

Key Vault

Trading Partner

Name \*

Certificate for Financial Transfers

Description

Financial transfers with trading partners

471 Characters Remaining

Algorithm \*

RSA

Size \*

2048

Password \*

.....

Confirm Password \*

.....

Store Password

Yes

Signature Algorithm \*

SHA256withRSA

Common Name \*

www.example.com

Organization Unit \*

Accounting

Organization \*

Example Company

Locality \*

Ashland

State \*

NE

Country \*

United States

Email Address \*

kharris@exmaple.com





Expires On \*


Mar 6, 2022

Subject Alternative Names

Add Name

Name	Value
No records found.	

- Click the  Action icon next to the desired Key Vault and select  Manage Certificates.
- In the Certificates page, click the  Import button in the toolbar.
- On the Import Certificate page, choose the Import From location where the certificate file is located:
  - Workstation - Click the Choose File button to select a file from your PC.
  - Server - Specify the location for the file or click the  Browse button to locate the file.
- Specify the File Format for the certificate. Depending on the file format selected, additional options may appear:
  - Certificate (.crt or .cer) - No additional options will appear.
  - PEM Key Pair (.pem) - Specify the password for the key pair and determine if the password will be stored in the Key Vault.
- Type an alias name to assign to the certificate. The name must not already exist in the Key Store.

8. Click the  Import button to import the certificate.
9. If the import is successful, the certificate(s) will load into the Key Vault and will be listed on the page.

	Name	Description	Subject	Issuer
<input type="checkbox"/>	testcert	testcert	10.1.3.253	AcumenCA

10. The product provides an option to leverage the uploaded certificates for each of the specific service in its own configuration page. The security administrator has the ability to specify the support of mutual authentication as per the requirement.

## 7 Secure Updates

- Checking for Current Version

The following are the steps the operator may follow to query the system for its currently running version:

1. On the MFT dashboard click the Help button and go to About.
2. The current version of the TOE is displayed.

- Check for Software updates and Installing Updates

The following are the steps the operator may follow to query the system for its currently running version:

1. On the MFT dashboard click the Help button and go to Check for updates.
2. New software updates if any are present with instructions to upgrade them.

Updates to the TOE are digitally signed and verified by the platform (Windows Installer or RPM Package manager) prior to installation. The TOE does not update itself, but rather relies on the platform package manager to install updates.

- TOE Delivery

The GoAnywhere's web-portal is available that allows the users to login to their account and download the TOE's installers/update software. The communication with the web portal enforces user authentication and HTTPS connectivity so that traffic is encrypted, and the TOE is securely delivered to the user.

Once all the prerequisites are completed, The Go Anywhere MFT application package was downloaded by the testing facility through the GoAnywhere's web-portal that required the testing facility to login to their account and download the TOE's installers/update software. It was further ensured that the communication with the web portal enforced user authentication and HTTPS connectivity so that traffic is encrypted, and the TOE is securely delivered to the testing facility. After installation, the testing facility placed a license request for which the Help systems personnel activated the license.

Note: A user account is needed to download the Go Anywhere MFT application package from the GoAnywhere's official website and by default it comes with 30 days free trial license with limited functionality. In order to obtain the complete functionality, a license request must be placed through the customer portal after user login for which the Help systems personnel will activate the license upon valid request.

## 8 TOE access to platform resources

Network connectivity is the only hardware platform resource accessed by the TOE. The TOE communicates with several IT environment for the following reasons. Database server for Remote database for storing settings and private keys, Authentication server for Remote authentication server for

user authentication, File server for Remote file server for storing user files, Mail server for supporting SMTP to send notifications and Remote browser for Remote administration and User file access. System logs are the only sensitive information repository accessed by the TOE. The TOE accesses system logs (i.e., Windows Event log) for the purpose of writing events to the logs.

## 9 References

The following documents were created and evaluated as part of the GoAnywhere MFT CC evaluation:

- Fortra's GoAnywhere Managed File Transfer v6.8 Security Target v1.1

End of Document